ملفات ساخنة (1)

حرب التحكم الآلي

سلاح الحرب الخامس









إصدار دار الجليل للنشر



اليازوري
دار اليازوري العلمية للنشر والتوزيع

ملفات ساخنة-1

حرب التحكم الآلي
سلاح الحرب الخامس

المملكة الأردنية الهاشمية
رقم الإيداع لدى دائرة المكتبة الوطنية
(2013/4/1352)

364.13
دار الجليل للنشر والتوزيع
ملفات ساخنة حرب التحكم الآلي سلاح الحرب الخامس/ دار الجليل للنشر والتوزيع.- عمان: دار الجليل للنشر والتوزيع، 2013
(203) ص.
ر.إ. : 2013/4/1352.

يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعّبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أخرى

الطبعة الأولى 2013

دار الجليل للنشر
والدراسـات والأبحـاث الفلسطينـية
هاتف:5157627-5155627
فاكس:5153668-عمان-الأردن
ص.ب 8972-رمز بريدي 11121
E-MAIL: darjaleel@gmail.com

دار اليازوري العلمية
للنشر والتوزيع
هاتف: 4626626 فاكس: 4614185
ص.ب 520646 رمز بريدي 11152
info@yazori.com
www.yazori.com



ملفات ساخنة-1

حرب التحكم الآلي
سلاح الحرب الخامس



الفهرس

مقدمة

تعمل دار الجليل على إعداد عدد من الدراسات التي تحمل عنوان "ملفات ساخنة"، فقد اخترنا أن يتطرق الملف الأول ويحمل عنوان "حرب التحكم الآلي-سلاح الحرب الخامس مصطلحاتها، أهدافها، انعكاساتها، والتعريف بميدان التحكم الآلي، والتعريف بـ"الهاكرز"-القراصنة- مثل سرقة بريد إلكتروني، سرقة فيس بوك، سرقة وشطب معلومات، حجب خدمات عن شركات الإنترنت، حالات الهجوم وعوامل كابحة في مجال التحكم الآلي، أهمية تكنولوجيا المعلومات ومجال التحكم الآلي المختلفة.

إننا نعرض الهجوم الذي شن على المفاعل النووي الإيراني، قبل سنوات، بإدخال فيروس "ستاكسنت" على هذا المفاعل، ضمن سلاح التحكم الآلي، إذ أشعل الضوء الأحمر لدى دول كثيرة، في حروب الظلال التي تجري اليوم بين الجيوش في عالم "السايبر"، وخاصة الجمهورية الإسلامية الإيرانية، التي قررت استثمار مبلغ مليار دولار، لتطوير وشراء تكنولوجيا معلوماتية بهذا الشأن، وتأهيل الخبراء الإيرانيين لتعزيز مقدرتها الدفاعية والهجومية في مجال التحكم الآلي.

وهـذا السـلاح يتـيح حتـى للأفـراد محاربـة دولـة وإحـراز نجـاح كبـير كقيـام أحـد السـعوديين باختراق مواقع إسرائيلية، وآخرون قاموا باختراق آلاف بطاقات الإئتمان الإسرائيليـة، لـيرد علـيهم الإسرائيليـون باختراق مواقع سعودية، والتعرف على بطاقات ائتمان، كما أن الفلسـطينيين قـاموا بـاختراق لمواقـع إسرائيليـة، سواء كانت للجيش، أو بعض الوزارات، وأجهزة أمنية، مما يتزايد الإدراك العام لصانعي القـرار في العديـد مـن

الدول، حول ضرورة الاهتمام بمجال "حرب التحكم الآلي"، للمواجهة والحماية في آن واحد، وبظننا أن هذا أول كتاب باللغة العربية يتطرق ويسلط الأضواء حول هذا الموضوع، والسؤال: هل سيأتي اليوم الذي ستختفي فيه المعدات والصواريخ والطائرات والدبابات، وتصبح الحرب عبر الإنترنت؟ بنظرنا كل شيء جائز والمخفي أعظم.

دار الجليل

الفصل الأول

حرب التحكم الآلي
مصطلحاتها وأهدافها

- مجال حرب التحكم الآلي يحتوى على ثلاثة عوامل يرتبط أحدها بالآخر:عامل إنساني وعامل منطقي وعامل مادي.

- أهم خصائص مجال الحوسبة هو مقدرة العمل بسرعة تقارب سرعة الضوء دون أية قيود جغرافية تقليدية.

- استخدام خصائص مجال الحوسبة يمكنه أن يقلص إمكانية الاكتشاف، ومعقولية الإدانة ومخاطر الرد المعاكس.

- مجال الحاسوب يتيح الفرصة للوصول إلى أهداف يصعب ضربها عبر الهجوم التقليدي

- الهجوم عبر التحكم الآلي غير مؤهل لحسم الأمور أو إحراز إنجازات إستراتيجية تعادل احتلال المناطق بأيدي القوات البرية بيد أنه مؤهل لإلحاق الأضرار بأهداف العدو الحيوية وبقدراته.

تمهيد:

تعتبر حرب التحكم الآلي بمثابة حرب جديدة ينضم ميدانها إلى ميدان الحروب البرية والبحرية والجوية والفضائية. وسوف نتطرق هنا إلى طبيعة هذه الحرب الخاصة، ومجالها، وسنقترح مصطلحات وتفسيرات جديدة لمصطلحات تقليدية،وسنستعرض الأحداث والاستعدادات التنظيمية في مجال حرب الحوسبة في إسرائيل والعالم.

تعمل الدول والجيوش المتطورة في العالم على زيادة معرفتها ونشاطاتها في مجال الحوسبة، والتي تعتبر بالنسبة لها مصدر قوة هائلة، وفي نفس الوقت نقطة ضعف. فعلى سبيل المثال فإن التجهيزات الحيوية لعمل الدولة – الكهرباء، الاتصال، المياه، المواصلات والمال وغيره- والتي يعتمد عليها هذا المجال، وشبكات القيادة وحرب التحكم الآلي العسكرية والتكنولوجية الحديثة المستخدمة في ميادين القتال العصرية رهن بهذا المجال أيضا.

ويمكننا أن نضيف إلى المجالات السابقة أيضا: أجهزة جمع المعلومات، إعداد وتصنيف وتحليل المعلومات، استغلال الأقمار الصناعية وميادين القتال، استخدام الآلات الحربية الخاصة، الدمج بين المجسات الحرارية الكاشفة للأهداف وبين وسائل الحرب في ميادين القتال وغيره.

هناك مميزات خاصة لمجال الحوسبة- مثله كمثل كل ميدان قتال- والتي تتيح فرصة العمل خلال أجزاء من الثانية ضد الأعداء على أبعاد هائلة جدا من الدولة ودون تعريض المقاتلين للأخطار. إن المزايا الخاصة المذكورة تجعل هذا المجال جذابا للحرب بما فيها خلال المراحل الواقعة بين الحروب التقليدية. ويمكننا أن نلاحظ المواجهات الدائرة في مجال الحوسبة – على غرار الهجمات التي شنتها روسيا على أستونيا عام 2007- وبين الحروب التي يعتبر فيها الهجوم في مجال الحوسبة بمثابة عامل في الحرب إلى جانب عوامل أخرى – مثل الهجمات التي شنتها روسيا على جورجيا عام 2008. كما أن بالإمكان التمييز بين الهجمات التي تجري في مجال الحوسبة – المساس بمنظومات الاتصالات والحاسوب- وبين استخدام هذا المجال كوسيلة

من أجل المساس بأداء الأجهزة العاملة في المجالات المادية. فعلى سبيل المثال فإن الهجوم في مجال الحوسبة على المشروع النووي الإيراني الذي وقع عام 2009، والذي هاجم خلاله فيروس ستاكسنت التجهيزات النووية أكد قوة "الأسلحة" في هذا المجال، واعتبر هذا الهجوم بمثابة حدث أساسي في تطور هذا المجال بوصفه ميدان حرب.

إن عددا من أحداث الهجمات في مجال الحوسبة، والإجراءات التي تتخذها الدول في هذا المجال تؤكد على أن سباق التسلح في هذا المجال قد بدأ فعلا، وفي إطار هذا السباق أنشئت مكاتب وهيئات خلال السنوات القليلة الماضية في دول مختلفة ممن تعمل على هذا المجال بوصفه ساحة حرب، وتمت بلورة إستراتيجيات عمل في الولايات المتحدة، بريطانيا، فرنسا، ألمانيا الصين وغيرها من الدول. ويبدو أن حرب التحكم الآلي ستحتل موقعا منذ الآن في كل حرب حديثة، هذا في الوقت الذي تقوم فيه تقديرات مانعة أمام الدول من خوض مثل هذه الحرب، مثل: الضبابية التي تلف نتائج هذه الحرب، والمخاطرة بالتعرض لهجومٍ مضاد في الوقت الذي لم تبن فيه مقدرة دفاعية كافية، هذا عداك عن أن الجهات الإرهابية قد تلجأ إلى خوض هذا المجال من أجل تنفيذ هجمات بعد أن تحصل على مقدرة يمكنها إلحاق أضرار جسيمة.

لقد بدأت تتطور مفاهيم دولية تنص على ضرورة العمل على حماية هذا المجال للصالح العام وترتيب العمل فيه على غرار ما هو معمول به في المجالات الأخرى، وذلك عبر التعاون بين الدول وملاءمة قواعد المجال الدولية، وبلورة ميثاق دولي ملزم. ومن الجدير بالذكر أن العمل على هذا الصعيد يتقدم ببطء شديد بصورة لا تتلاءم ووتيرة تطور مجال الرقابة والسيطرة.

أسهمت تكنولوجيا المعلومات ومجال حرب التحكم الآلي في إسرائيل إسهاما حاسما على صعيد التفوق النوعي الإسرائيلي في المجالين الأمني والاقتصادي. إن مجال الحوسبة هو مجال شديد الحيوية بالنسبة للمجتمع، وللصلة القائمة بين الحكومة والمواطنين والصلة بين إسرائيل والعالم، بل إن لهذا المجال أهمية كبيرة جدا بالنسبة للأمن القومي الإسرائيلي آخذين بعين الاعتبار التهديدات الآخذة بالتبلور في هذا المجال،

وبالتفوق الذي تتمتع به إسرائيل في مجال تكنولوجيا المعلومات والاحتمالات التي يوفرها مجال الحوسبة في ميـادين القتال العصرية.

لقد قام الجيش الإسرائيلي بخطوة هامـة عـام 2009 باعترافـه بمجـال الحوسـبة بوصـفه مجـالا إسـتراتيجيا وعمليا جديدا، ثم قيامه بإنشاء "هيئة الرقابة والسيطرة" التابع لهيئة الأركـان العامـة لتنسـيق وتوجيـه نشـاطاته في المجال – وهي خطوة مماثلة لتلك التي قامت بها الولايات المتحدة في نفس المجال في وزارة الدفاع الأميركية. وعلى ما يبدو فإن المصطلحات التقليدية الإسرائيلية المتعلقة بنظرية الأمن لم تعد تلائم مجـال الحـرب الجديـد، مـما يقـتضي تعديلها أو تطوير مصطلحات جديدة أكثر ملاءمة. فعلى سبيل المثال تختلـف "البيئـة الإسـتراتيجية" في مجـال حـرب التحكم الآلي عن المصطلح المقبول في إسرائيل والذي يقوم على دوائر التهديد الجغرافية التقليديـة. إن التعامـل مـع "الوقت والمجال" في مجال حرب التحكم الآلي مختلف، نظرا لأن سرعة العمليـات فيـه تقـاس بـآلاف الجزئيـات مـن الثانية. إن مجال حرب الـتحكم الآلي يعـزز مقـدرة العـاملين الحـاليين، ويتـيح الفرصـة لعـاملين جـدد للإعـراب عـن مقدرتهم الهجومية في هذا المجال – وخصوصا من الأشخاص الذين لم يسبق أن شاركوا في معارك سابقة بسبب القيود الجغرافية والسياسية أو تدني المقدرة العسكرية التقليدية.

أما على صعيد نظرية الردع، والتي تحتل المرتبة الأولى في نظريـة الـدفاع التقليديـة الإسرائيليـة، فـإن مـن الصعب تطبيقها في هذا المجال بسبب صعوبة اكتشاف الجهة المسؤولة عن الهجوم، الأمر الـذي يجعـل مـن الصـعب بلورة وتنفيذ سياسة رد رادعة. أضف إلى ذلك أن التاريخ القصير للهجوم في مجال حرب التحكم الآلي لم يتح الفـرص لوضع صورة "لرد الفعل" الناجع والرادع، ولا شك أن الحصول على مقدرة ردع تتطلب الكشف عن مقدرة حساسة في هذا المجال الأمر الذي قد يفقدها قيمتها.

وفي مجال الدفاع يعتبر الدفاع بمثابـة تحـد جديـد في مجـال الرقابـة والسـيطرة، حيـث أن بمقـدور العـدو تنفيذ هجماته بسرعة البرق ومن الصعب اكتشاف المهـاجم. وبمقـدور إسرائيـل أن تـتعلم شـيئا مـا بهـذا الخصـوص

من التجربة الأميركية "للدفاع الفعال"، والتي تقوم على المقدرة الاستخبارية المتقدمة لاكتشاف أية نشاطات في الشبكات، والاعتماد على تجهيزات آلية لاكتشاف الهجمات والرد بصورة أوتوماتيكية دون تدخل بشري، ومقدرة الهجوم الوقائي. وتجدر الإشارة إلى أن الدفاع الفعال لا يقوم على تكنولوجيا متقدمة فقط بل أيضا على تخطيط شبكة عمل فعالة، وإجراءات وثقافة، ومعرفة الأخطار والانضباط الشديد، وحماية مادية ورقابة إنسانية.

الإنذار الاستخباري: يختلف الإنذار الاستخباري في مجال حرب التحكم الآلي مقارنة به في الحروب التقليدية. حيث أن الاستعدادات لشن هجوم في مجال حرب التحكم الآلي تجري في غرف مغلقة وبواسطة طواقم صغيرة وسرية بعيدا عن الهدف، لذا من الصعب توقع تسرب معلومات مسبقة لاستخدامه كقاعدة للتحذير، هذا مقارنة بالاستعدادات الخاصة بشن الحروب التقليدية. بل إن من الصعب في بعض الحالات أن نعرف في الوقت المناسب أن الحرب قد بدأت فعلا، لقد تم تنفيذ جميع الهجمات في مجال حرب التحكم الآلي حتى الآن بصورة مفاجئة تماما.

لقد أعلن رئيس الحكومة الإسرائيلية بنيامين نتنياهو في الثامن عشر من أيار 2011 عن إنشاء "هيئة حرب التحكم الآلي القومية". وبناء على بيان مكتب رئيس الحكومة، فإن الهدف المركزي لهذه الهيئة هو توسيع مقدرة الدفاع الإسرائيلية عن المنظومات الحيوية في البنية التحتية الإسرائيلية من الهجمات الإرهابية في مجال السيطرة والرقابة، سواء كانت التي تقوم بها دول أجنبية أو جهات إرهابية. وسوف يتم إنشاء هذه الهيئة إضافة إلى الجهات الرسمية والعملية المدنية العاملة في هذا المجال مثل: الهيئة الحكومية لحماية المعلومات في جهاز الأمن العام، ومشروع خطة التعليم الأساسي للدراسات العليا، والتي تقدم خدمات انترنت محمية للوزارات والمؤسسات الحكومية.

يبدو أن التحدي المركزي الذي يواجه هيئة حرب التحكم الآلي القومية المستقبلية يتمثل في خلق منظومة دفاع قومية صلبة في مجال السيطرة والرقابة، ولا شك أن هذه المهمة تشذ عن مهمة الدفاع عن البنى

القومية الحساسة والتقليدية، ولا شك أنها أيضا ذات مستوى رفيع وشديد التعقيد. وعلى خلاف مجالات الحرب الأخرى، بل وحتى مجال الهجوم في مجال حرب التحكم الآلي التي تديرها وزارة الدفاع الإسرائيلية، فإن إنشاء منظومة دفاع فعالة في هذا المجال يتطلب تعاوناً بين الوسط المدني والوسط الأمني نظرا لصعوبة الفصل في العديد من المجالات بين البنى في مجال حرب التحكم الآلي المدنية والعسكرية. كما أن هناك حاجة للتعاون بين القطاع العام – الجيش والقطاع المدني- والقطاع الخاص، نظرا لأن قسما كبيرا من المقدرة في مجال حرب التحكم الآلي موجود في أيدي القطاع الخاص، مثل الشركات التكنولوجية الفعالة، وشركات الاتصالات، وشركات الحماية، وشركات البنى الحيوية وغيرها. كما أن هناك ضرورة للتعاون مع دول أخرى، حيث أن إمكانية استخدام شركات مراقبة وتعاون استخباري مشتركة يمكنها أن تحسن قدرة الإنذار، وقدرة مراقبة ومتابعة مسارات الهجوم، واكتشاف مصادرها وتحديد قدرة الرد عليها.

وعلى ضوء كل ذلك فإن مهمة هيئة حرب التحكم الآلي القومية تتضمن المهام التالية:

أ-مساعدة الكادر السياسي في اتخاذ القرارات وبلورة السياسات لحماية مجال حرب التحكم الآلي القومي، بما فيها بلورة اقتراحات للعمل بإستراتيجية قومية لحماية مجال حرب التحكم الآلي بالتعاون مع الجهات ذات العلاقة التي سيصادق عليها المجلس الوزاري الأمني والسياسي.

ب- تقدير الأخطار: أخطار شاملة ومؤقتة بالاعتماد على المعطيات والتقديرات التي تقدمها الجهات الاستخبارية والتكنولوجية ذات العلاقة.

ت- تقديرات الوضع: شاملة ومؤقتة، بما فيها التوصيات للعمل على بناء التحليلات البديلة.

ث- التعليمات الإستراتيجية للجهات المدنية المشاركة في حماية مجال السيطرة والرقابة، والتنسيق مع الجهات في الوسط الأمني.

ج - تنسيق العمليات لجميع الجهات الحكومية والخاصة ذات العلاقة بأمن مجال السيطرة والرقابة، بما فيها تحميل المسؤولية للوزارات الحكومية والمدنية من أجل العمل على تحسين أمن السيطرة والرقابة، كل في مجالها.

ح- إنشاء مركز إداري وتنفيذي لمجال حرب التحكم الآلي على أن تتمثل مهمته في خلق صورة وضع ديناميكي بشأن التهديدات في هذا المجال، والتعاون في تبادل المعلومات مع جميع الجهات ذات العلاقة بالأمر وتقديم المساعدة في مجال إدارة عملية الحماية.

خ- تحديد منظومات البنى التحتية والجهات المدنية التي يتوجب على الدولة توجيهها أو حمايتها في مجال حرب التحكم الآلي وفقا للإستراتيجية القومية.

د- المبادرة إلى سن تشريعات وأنظمة حيوية للعمل من أجل حماية مجال حرب التحكم الآلي في أوقات الطوارئ والأوقات العادية.

ذ- طرح مبادرات وقيادة مشروعات حكومية مثل مشروعات تحسين أساليب ووسائل الدفاع عن منظومات المعلومات – بما فيها الحماية المادية، تشكيل منظومات توجيه للعاملين في القطاع الحكومي، العمل على تحسين قدرة الترميم في أعقاب التعرض لهجوم في مجال السيطرة والرقابة، إدارة مناورات دفاعية في مجال التحكم الآلي على المستوى القومي.

ر- تحديد معايير للتطوير، والمشتريات وتركيب المعدات الخاصة بالاتصالات والحوسبة في ذات المجال.

ز- منح تصاريح لإقامة بنى تحتية للاتصالات والحوسبة فيما يتعلق بتأثيرها على أمن مجال حرب التحكم الآلي القومي.

س- المبادرة والتوجيه في مجال تطوير وسائل الحماية، والتأهيل للطاقة البشرية المهنية والأبحاث العلمية بشأن حماية مجال السيطرة والرقابة، بما فيها منح محفزات للجهات العاملة في مجال الأبحاث.

ش- المبادرة إلى عمليات تعاون إستراتيجية بين القطاع الحكومي والقطاع الخاص، بما فيها التعاون مع شركات اتصالات وتكنولوجية في المجال التشغيلي والأبحاث والتطوير.

ص- تركيز التعاون مع الدول الأخرى في مجال أمن مجال السيطرة والرقابة.

ض- الرقابة على التطبيقات الإستراتيجية وعلى النشاطات لحماية مجال السيطرة والرقابة، والتأكد من وجود رقابة مناسبة على الوزارات الحكومية المختلفة والسلطات المدنية، والرقابة على مصادر الاتصالات بالنسبة للتجهيزات والتطبيقات العامة وأمن مجال السيطرة والرقابة.

ط- تحسين قدرة السكان على حماية أنفسهم، والرقابة على مستوى الخدمات المختلفة التي تقدمها الجهات التي تقدم الاتصالات وشركات الحماية للجماهير.

ظ- تشكيل مركز معلومات قومي في مجال حماية مجال حرب التحكم الآلي والمرتبط بمراكز معلومات في إسرائيل والخارج، وتعلم أساليب المواجهة التي تستخدمها الدول الأخرى لمواجهة تحديات حرب السيطرة والرقابة.

إن بمقدور إسرائيل إن تكون دولة رائدة في العالم على صعيد حماية مجال السيطرة والرقابة، إزاء "رأس المال البشري" والمعلومات التكنولوجية الرفيعة التي تتحلى بها، ولا شك أن استنفاد هذه الطاقات يمكنه أن يسهم في تحسين مكانة الدولة على الصعيد الأمني والاقتصادي.

إسرائيل كمدخل :

اكتشفت منظومة إنذار حرب التحكم الآلي الإسرائيلية هجوما "بقنابل برنامج حاسوب" على محطتي طاقة إسرائيليتين، فقامت المجسات الحرارية بصورة فورية وبسرعة البرق بتفعيل جهاز الاعتراض،الذي قام بدوره بالقضاء على غالبية المهاجمين، بيد أن قسما من "القنابل" تمكن من اختراق جهاز الدفاع وضرب جهاز الرقابة في إحدى المحطتين، الأمر الذي ألحق أضرارا بالبرامج لكن ولحسن الحظ فإن تلك الأضرار لم تصل إلى المجالات المادية. وقد قام جهاز الحماية فورا بالتشغيل الآلي لمنظومة Roll Back في المحطة والتي أعادت في غضون جزء في الألف من الثانية عمليات الحاسوب إلى الوراء، إلى الوضع الذي كان عليه قبل اختراق القنابل. ومن الجدير بالذكر أن مجال حرب التحكم الآلي هو المجال الوحيد الذي يتيح إمكانية العودة بالزمن إلى الوراء إلى حالة العمل السابقة. ثم وفي نفس الوقت عملت المنظومة على قطع التيار الكهربائي، الذي يوقف عمليات منظومات الاتصالات والحوسبة في الأهداف المدنية الحيوية التي تم تحديدها مسبقا.

لقد نجح الدفاع الجوي الإسرائيلي في نفس الوقت باعتراض صاروخ بالستي وجه إلى مزرعة خدمات شركة التليفونات القومية، وبذلك تم إنقاذ مجال حرب التحكم الآلي السياسي والذي يمكننا القول إن وجوده منوط ببنية خدمات الاتصالات وبالطاقة الكهربائية. ورغم ذلك فإن شركة التليفونات التي تقدم خدمات الاتصالات الشخصية – تليفونات خلوية واتصالات بالأقمار الصناعية- أصيبت بأضرار جسيمة مما شوش عمل الجيش بصورة أكثر خطورة مما كان يتصور.

إن هذه الأحداث كانت جزءا من السيناريوهات التي تمت دراستها في المناورة القومية التي ستجري في إسرائيل عام 2016. وقد وصفت المناورة بأنها بمثابة نجاح كبير. لقد طرأ خلال السنوات القليلة الماضية تحسن كبير على مهام ووظائف أجهزة الحماية السياسية في نقل المعلومات بين الجهات المختلفة وفي التنسيق بين الأجهزة المدنية والعسكرية. ورغم ذلك تم التأكيد على أن منظومة الدفاع القومية تزويد إسرائيل بردود لحماية

البنى القومية الحيوية والأجهزة الأمنية بيد أنها لا تزود إسرائيل بردود كافية للقسم الأكبر من مجال حرب التحكم الآلي السياسي الذي يملكه القطاع الخاص.

وفي تعليقه قال رئيس الحكومة الإسرائيلية نتنياهو إبان دراسة المناورة: إن من حق جميع مواطني الدولة توفير الحماية لهم وتوفير حرية العمل في مجال حرب التحكم الآلي مثلما توفر الدولة الحماية في المجالات الأخرى. وبناء عليه اتخذ قرار بتركيب منظومة حماية على التجهيزات الخاصة بالدخول إلى الدول الكترونيا تقوم على التأخير للحظات لوسائل الاتصالات الداخلة (delay line) بحيث تتاح الفرصة لعمليات الإحباط وتفعيل منظومة Roll Back على المستوى القومي.

إن هذا السيناريو ليس مجرد توقع، بل لقد خطط كي يكون تجسيدا لمجال حرب التحكم الآلي والتحديات الكامنة فيه أمام إسرائيل.

مجال حرب التحكم الآلي

والمجالات الأمنية...أطر ومصطلحات

يصف مصطلح "مجال السيطرة والرقابة" ظاهرة بدأت عندما تم تطوير التلغراف عام 1844، والتي تقوم على استغلال الحقول الالكترونية للاحتياجات الإنسانية عبر التكنولوجية. وتعتبر نقطة التحول الرئيسية والجوهرية في تطور هذا المجال، عندما تم تطوير الحاسوب الرقمي عام 1949، ثم كانت هناك معالم طريق أخرى مثل: الربط بين شبكات الاتصالات وبين الحواسيب والآلات والذي بدأ في السبعينات، الاستخدام الواسع لشبكة الانترنت والحواسيب الشخصية في منتصف التسعينات، الجمع بصورة شاملة بين منظومات الحاسوب وأجهزة الاتصالات والآلات على اختلاف أنواعها – في الصناعة والمواصلات وغيرها، استخدام واسع للحواسيب الشخصية الصغيرة، ازدهار الشبكات الاجتماعية في الانترنت وغيرها خلال العقد الماضي. وقد أسهمت كل هذه العوامل في تغيير وجه المجتمع والاقتصاد.

إن تكنولوجيا المعلومات ومجال حرب التحكم الآلي يعملان على إحداث تغيير سريع أيضا في طبيعة ميادين القتال العصرية، وليس أدل على ذلك من نموذج التكنولوجيا العصرية في ساحات القتال مثل: أجهزة الإدراك، التعاون في مجال المعلومات،تحليل المعلومات، استغلال الأقمار الصناعية في ميادين القتال، تفعيل وسائل أوتوماتيكية، الدمج بين المجسات الكاشفة للأهداف والمنظومات النيرانية وغيره. لقد أدى تطور مجال حرب التحكم الآلي إلى تمكن القطاعات المدنية من استعراض ساحات القتال بواسطة أجهزة خلوية متحركة والتي تمنح كل شخص موجود في المنطقة القدرة على توثيق المعلومات والتي يتم نقلها فورا عبر الانترنت، مما يثير نقاشات في الشبكات الاجتماعية ويؤثر على الرأي العام. وهكذا تحولت ساحات القتال إلى مناطق تلعب فيها الجماهير دورا مركزيا، وتؤثر أكثر من السابق على سياسة الحكومات والمؤسسات الدولية، وفي بعض الأحيان بناء على معلومات هادفة.

ولا شك أن لهذه الظاهرة مغزى بعيد المدى في كل ما يتعلق باستخدام القوة العسكرية، فهـي تحـد مـن قدرة استخدام القوة، بيد أنها قادرة أيضا على المساهمة في تجنيد الرأي العام لصالح استخدام القوة.

محددات:

هناك عدد من المحددات والأوصاف ذات العوامل المشتركة لمجال السـيطرة الإداريـة. لقـد وصـفت وكالـة الأمم المتحدة **International Telecommunication Union** مجال حرب التحكم الآلي على النحو التالي: المجـال المادي وغير المادي المتولد أو المركب من قسم أو من جميع العناصر التالية: الحواسيب، المنظومات الآلية والشبكات، برامج الحاسوب، المعلومات المحوسبة، المحتوى، معطيات النقل والرقابة وجميع أولئك الذين يستخدمونها.

ويتضح من هذا الوصف والتحديد أن مجال حرب التحكم الآلي يحتوى على ثلاثـة عوامـل يـرتبط أحـدها بالآخر:

أ- عامل إنساني: مستخدمو وسائل الاتصالات والحواسيب.

ب- عامل منطقي: عامل البرامج التي تتحرك بسرعة الضوء وتقدم معلومـات، إجـراءات، ومـواد سـيطرة ورقابة - مثل "البرامج ذات القيمة الكبيرة، والأموال الالكترونيـة – والـبرامج الشريـرة - مثـل حصـان طروادة وغيره.

ت- عامل مادي: المركبات المادية للشبكة: مواد، بنية متحركة وثابتة في المجالات البرية والبحرية والجوية والفضائية

وهناك أوصاف وتحديدات أخرى لمجال السيطرة والرقابة، وهي جميعا تتعلق بالعوامل الثلاثة التي أشرنـا إليها: الإنساني، والمنطقي والمادي. وكل عامل منها يصف مجال حرب التحكم الآلي عبر قسم من العوامل فقط .

وتعرف وثائق الجيش الأميركي مجال حرب التحكم الآلي باستخدام العامل الثاني – العامل المنطقي، والثالث – المادي على النحو التالي: "مجال عالمي داخل محيط المعلومات مركب من شبكات تستند على بنى تكنولوجيا المعلومات الممتزجة الواحدة بالأخرى بما فيها الإنترنت وشبكات الاتصالات، ومنظومات الحواسيب، والمعامل والرقائق والرقابة". ويفيد التعريف الأميركي أيضا إن مجال حرب التحكم الآلي هو المجال الخامس – إضافة إلى المجال البري، الجوي، البحري والفضائي- وأن هناك علاقة تبادلية بين هذه المجالات الخمسة، حيث أن مجال حرب التحكم الآلي مزروع في كل مجال من المجالات الأخرى، ويقوم بعملية الربط بينها وتعزيز مقدرة العمل فيها.

لقد وصف مجلس الوزراء البريطاني في مستند إستراتيجي تحت عنوان "بريطانيا لحماية أمن السيطرة والرقابة" مجال حرب التحكم الآلي على النحو التالي: مجال يشمل جميع صور شبكات الاتصالات والنشاطات الرقمية بما فيها النشاطات والبرامج التي يتم تناقلها عبر شبكات الاتصال الرقمية". ولا شك أن هذا الوصف وضع العامل المنطقي على رأس قائمة الفهم.

ووصفت وزارة الداخلية الألمانية في وثيقة "الإستراتيجية الألمانية لأمن مجال السيطرة والرقابة" هذا المجال بصورة مقلصة نسبيا كما يلي: "مجال جميع أنظمة المعلومات المرتبطة فيما بينها على المستوى العالمي. إن الانترنت هو الأساس لمجال حرب التحكم الآلي بالإضافة إلى شبكات المعطيات الأخرى." وبناء على هذا الوصف فإن منظومات المعلومات المنعزلة ليست جزءا من مجال السيطرة والرقابة.

وعلى عكس التعريف الذي يرى في مجال حرب التحكم الآلي مجالا خامسا، هناك اتجاه يقول إن مجال حرب التحكم الآلي هو أحد سبعة مجالات إلى جانب المجال الجوي والبري والبحري والفضائي، والمجال الإلكترو-مغناطيسي والمجال الإنساني. إن هذا الاتجاه يميز بين مجال حرب التحكم الآلي وبين المجال الإلكترو- مغناطيسي ويعتبر المجال الإنساني بمثابة مجال قائم بنفسه.

إن مجال حرب التحكم الآلي هو مجال مصطنع يتم تجسيده بواسطة المجال الإلكترو- مغناطيسي ويتصل مع المجالات المختلفة الأخرى بواسطة مجسات ومؤثرات، ومن ثم فإن مجال حرب التحكم الآلي يستخدم لتعزيز عمل المنظومات المدنية والعسكرية العاملة في جميع المجالات وفي نفس الوقت فإنه يعرضها لهجمات السيطرة والرقابة.

إن القاسم المشترك الواضح بين جميع الأوصاف السابقة هو العامل المنطقي. إن التغيير في الأوصاف بين التعريفات المختلفة يعكس، على ما يبدو، الجوانب التي تهتم بها كل دولة ومنظمة في محاولاتها مواجهة التحديات في مجال السيطرة والرقابة. ويبدو أن الفروق في الأوصاف والتعريف لا تعكس فهما مختلفا لمجال السيطرة والرقابة، نظرا لأن جميع أصحاب الأوصاف يعترفون بوجود العوامل الثلاثة التي أشار إليها تعريف الأمم المتحدة.

الجدول رقم 1: عوامل مجال حرب التحكم الآلي الثلاثة:

العامل	نوع العمل في العامل والهدف	المحتوى"نماذج"	هدف التطوير "نماذج
1-عامل المستخدم أ- العامل الإنساني --------------------------- 2- العامل المنطقي أ- مجال الاستخدام الجرافيكي (GUI) ------------------------- ب- برامج التطبيق	استخدام إنساني لوسائل الاتصال والحاسوب ------------------------ عمل برامج ترجمة معلومات من لغة المستخدم إلى لغة الحاسوب (معلومات رقمية)والعكس ------------------------- إعداد المعلومات التي تصل من مجالات المستخدم، برامج إدارة شبكات	قراءة، تجارة، استثمارات، استخلاص معلومات، تبادل معلومات، اتصالات مع أصدقاء، صلة بين مدنيين والوزارات الحكومية، جريمة وحرب سيطرة ورقابة أوراق، صيغ، صور، أفلام، سماعي ، أزرار تفعيل	زيادة في ظاهرة جماعات المستخدمين، واستخدام أجهزة متحركة والتليفونات الذكية، وبداية استخدام شبكةWEB3 ------------------------- ارتفاع في أنواع ومستويات الانعكاسات المعروضة في المجال، ارتفاع في التمثيل الجرافيكي أكثر من D3 ---------------------- انعكاسات أكثر، أكثر وأكثر عوامل برمجة بين المواد ومجال المستخدم.

3- العامل المادي			
أ- المواد	بنية مادية إلكترو- مغناطيسية تقوم بتنفيذ عمليات	أوامر وإعدادات تدفق بلغة البرمجة رقائق، بطاقات إلكترونية وغيره، تيارات كهربائية	زيادة في حجم المعلومات حول المركبات الإلكترونية، تصغير، متحرك، وذاكرة ضوئية -رقيقة تقوم بالاحتفاظ بالمعلومات دون توتر كهربائي.
ب- منظومة اتصالات وطاقة (بنية الكترونية)	توفر شروط وجود وعمل أجهزة الاتصالات والحوسبة في المجال الإلكتروني	بنية وصيانة، نشر كابلات وأحرف RF وموجات ضوئية وكهربائية	زيادة في أنواع وانتشار منظومات الاتصالات والاتصالات الخلوية، راوتر، أقمار صناعية، كابلات بحرية، تحسن استغلال الطاقة
جـ- وسائل حاملة للمواد والبرامج	توفر شروط أخرى لتواجد مجال حرب التحكم الآلي في المجال البري، البحري الجوي والفضائي		حواسيب وتليفونات ذكية، منشآت، منظومات ومعدات تم تركيب حواسيب فيها، تجهيزات تم تركيب معامل ورقابة عليها، وسائل تحمل معدات تسجيل ، مجسات ومؤثرات. في هذه المنطقة تجري عمليات الاتصال بين مجال حرب التحكم الآلي وبين المجال المادي.

خصائص مجال حرب التحكم الآلي كساحة حرب

هناك أنواع من العمل الأمني المتعلق بمجال حرب التحكم الآلي في كل نوع من أنواع العوامل الثلاثة (الإنساني، المنطقي، والمادي) التي أشارت إليها الأمم المتحدة. وعلى سبيل المثال:

أ- عمليات في مجال حرب التحكم الآلي الموجهة إلى العامل الإنساني، والرامية إلى تغيير مسلكية الإنسان المستخدم. ومن بينها نقل رسائل معلوماتية – علنية أو سرية- إلى الخصم بواسطة مجال حرب التحكم الآلي .

ب- اختراقات منطقية – بواسطة البرامج- لأهداف كالتجسس، مهاجمة حواسيب الخصم من أجل منعه من الحصول على الجدوى من الحاسوب،ومهاجمة تجهيزات ومنشآت في المجالات المادية التي تسيطر عليها الحواسيب. وعلى سبيل المثال تشويش أجهزة الرقابة الحرارية مما سيؤدي إلى تفجير معمل أمني وتأثيراته على المجال البري. أو تشويش معايير الارتفاع التي ستمس بوسائل الطيران – تأثير في المجال الجوي. ومن الجدير بالذكر أن مجال الحاسوب الخاص بالخصم يتحول في هذه الحالة لخدمة المهاجم، مما يجعله يحرص على عدم الإضرار به.

ت- العامل المادي: المساس بالمادة التي يعتمد عليها العامل المنطقي، وكذلك القيام بعمليات خارج مجال الحوسبة ضد البنى التي يعتمد عليها المجال. مثل العمل عبر الحرب الالكترونية والتي ترمي لضرب أو إسكات عوامل الاتصال ومنظومات الطاقة ذات الصلة بمجال الحوسبة.

ويمكننا أن نتعرف على خصائص مجال الحوسبة من تطرق كبار الشخصيات في الجهاز الأمني الأميركي، ومن ضمنها المقالة التي كتبها وزير الدفاع الأميركي وليام لين في آب 2010 تحت عنوان "إستراتيجية وزارة الدفاع في مجال الحوسبة". والشهادة التي أدلى بها الجنرال كايت ألكسندر في نيسان 2010 أمام الكونجرس. كما أن بالإمكان أن نتعرف عليه من الوثائق الرسمية التي نشرتها المؤسسات الأمنية في الولايات المتحدة وأوروبا ، ومن المقالات الأكاديمية والتصريحات التي يدلي بها الخبراء والشخصيات الرفيعة في وسائل الإعلام.

وبناء على المعلومات من تلك المصادر وتحليل الأحداث سوف نستعرض فيما يلي خصائص ساحة الحرب الجديدة "مجال الحوسبة":

مقدرة عمل بسرعة تقارب سرعة الضوء دون أية قيود جغرافية تقليدي:

إن هذه الخاصية تسمح للمهاجمين تنفيذ هجومهم على أبعاد شاسعة وبسرعة البرق ودون أية احتكاكات مع الخصم في المجالات المادية. ورغم ذلك فإن مجال الحوسبة يرتكز على نشر بنية الشبكة. وإضافة

إلى عملية الدفاع، فإن المقدرة على شن الهجوم الخاطف يتطلب توفير منظومات دفاع حيوية قادرة على الرد الأوتوماتيكي ضد المهاجمين في الوقت المناسب ودون تدخل البشر.

مقدرة عمل سرية:

تشير العبر المستقاة من الهجمات التي جرت حتى الآن في مجال الحوسبة والمعلومات الخاصة بإستراتيجية العمل في مجال الحوسبة أن لدى المهاجم مقدرة للعمل في مجال الحوسبة بسرية ودون ترك أية آثار تدل عليه، والاستتار خلف عوامل أخرى مثل قراصنة الحاسوب، والجهات النائية، والمنظمات والدول الأجنبية. أي أن استخدام خصائص مجال الحوسبة يمكنه أن يقلص إمكانية الاكتشاف، ومعقولية الإدانة ومخاطر الرد المعاكس. وليس أدل على ذلك أنه وفي جميع الهجمات التي وقعت في مجال الحوسبة حتى الآن لم يكن بالإمكان تجريم الدولة المشبوهة. وذلك على عكس الحرب التي تدور في ساحة الحرب الحركية حيث يبدو بوضوح فيها من هي الجهة التي بدأت الحرب، ومن الجهة التي ألحقت الأضرار، والمنطقة التي تم احتلالها وغيره، وهو الأمر الذي لا يبدو أبدا في مجال حرب الحوسبة.

إن جميع هذه العوامل تعكس أبعادا متناقضة: فهي تسهم في كبح جماح ردود الفعل – نظرا لعدم معرفة الجهة التي يجب الرد على هجومها، وفي نفس الوقت هناك فرصة لتصعيد غير مراقب. فإذا وقعت على سبيل المثال هجمات أوقعت أضرارا جسيمة في الممتلكات والأرواح سوف تمارس ضغوط سياسية للرد على المشبوهين بالقيام بالهجوم حتى لو لم تتوفر أدلة قوية تجاه هوية المهاجم.

يمكن استخدام أسلحة الحاسوب كأسلحة غير قاتلة. إن القدرة على التسبب بإلحاق أضرار جسيمة في أداء الدولة دون تخريب بنيتها المادية أو قتل سكانها يعتبر بمثابة ميزة من المزايا التي تتمتع بها أسلحة الحاسوب مقارنة بالأسلحة المستخدمة الأخرى في مجال الحركة – الأسلحة النيرانية. هذا رغم أن بالإمكان إلحاق أضرار جسيمة عبر شن هجوم محوسب بالممتلكات والبشر بواسطة ضرب التجهيزات المرتبطة بمجال الحوسبة في المجالات المادية.

إن مجال الحاسوب يتيح الفرصة للوصول إلى أهداف يصعب ضربها عبر الهجوم التقليدي مثل:

أ- منشآت وأجهزة – وسائل اتصال، سيطرة ورقابة وغيره- موجودة في مناطق وعرة ويصعب مهاجمتها عمليا بسبب البعد، الدفاعات القوية، التجمعات السكانية وغيره.

ب- أفرع البنوك والمؤسسات المالية، وهي المؤسسات التي تعتبر في عصرنا بمثابة مؤسسات قومية شديدة الأهمية ومعرضة للهجمات في مجال الحوسبة، سواء كان ذلك بسبب الاعتماد الكبير للدول على المؤسسات المالية أو لارتباط هذه المؤسسات بمجال الحوسبة. إن المساس بالمؤسسات المالية يمكنه على سبيل المثال أن يحول دون نقل الأجور، والحد من التجارة الخارجية بل ويعطل الاقتصاد.

ت- منظومات لوجستية ومواصلات والتي ترتبط اليوم ارتباطا وثيقا بالحواسيب.

ث- معلومات متعلقة بمعطيات الدولة: الوزارات الحكومية، الجهاز القضائي والجامعات وغيره.

أخطار ضئيلة على حياة البشر:

تشتمل حرب التحكم الآلي على أخطار ضئيلة لحياة البشر المهاجمين مقارنة بالهجمات العسكرية التقليدية، والتي تعتبر مسألة تعريض حياة المهاجم للخطر بمثابة أحد التقديرات التي قد تحول دون شن الهجوم. وينطبق هذا الوضع أيضا على المدافع.

إن هذه الميزة تمنح الجانب المدافع حرية عمل كبيرة جدا بل وقدرة على استخدام وسائل أوتوماتيكية ضد الهجوم ودون تدخل البشر فيها ودون المخاطرة بالمساس بحياة البشر سواء كان ذلك في جانب المهاجم أو المدافع، وذلك على عكس الهجمات التقليدية بالأسلحة. كما أن الميزة المذكورة تجعل المهاجم أكثر جرأة في طرح وتنفيذ الأفكار الهجومية.

انتقائية:

إن هذا الجانب لا يأتي بصورة قاطعة، حيث أن بالإمكان – في حالات معينة – مهاجمة أهداف محددة في منطقة معينة دون المساس بأهداف أخرى. لكن إذا أخذنا بعين الاعتبار خصائص الهجوم التقليدي سنجد أن من الصعب السيطرة على معايير الهجوم وحجمه، ومن الجائز أن ينتشر الهجوم إلى مدى أوسع مما خطط له.

فيروس:

تميل الخاصية التي أشرنا إليها إلى أخذ صورة "فيروس" وتكييف نفسها بصورة متواصلة عداك عن قدرتها على التحرك في الشبكة إلى أماكن شتى. إن هذه الخاصية هي تحد صعب على المدافع، والذي يتوجب عليه العمل على منع انتشار الفيروس إلى مناطق مختلفة. ولا شك أن هذه الخاصية تعتبر بالنسبة للمهاجم بمثابة ميزة في حالات معينة من الهجمات الموسعة، حيث أن بمقدوره، باستخدام جهد محدود، خلق تأثيرات واسعة النطاق، ورغم ذلك يمكن لهذه الخاصية أن تشكل صعوبة للمهاجم المعني بشن هجوم موضعي وانتقائي والسيطرة الدقيقة على نتائج الهجوم.

معيارية مجال الحاسوب:

يقوم المجال بصورة أساسية على بنية شركات عالمية -ميكروسوفت، سيسو، تشيك بوينت وغيرها- والتي تتصل الواحدة بالأخرى وتتواجد في جميع الدول. إن الطابع العالمي لهذا المجال واستخدام نفس التجهيزات على سبيل المثال في التفعيل يخدم حقا أولئك العاكفين على بناء مجال الحاسوب بيد أن هذه يخلق أيضا أخطارا جسيمة على المدافع، فاقتحام برامج حماية معلومات معروفة أو مخزن معلومات تكنولوجية معين تابع لشركة حاسوب عالمية يمكنه أن يعرض جميع الأماكن التي يقوم مستخدمون باستخدام هذه المواقع. ففي آذار 2011 أعلنت شركة حماية المعلومات آر.إس.إيه التي تملكها شركة تخزين المعلومات العملاقة "إي.إم.سي" أنها تضررت جراء تعرضها لهجوم قراصنة حاسوب والذين نجحوا في سرقة معلومات تتعلق

بالحماية والمستخدمة للتأكد من هوية عمال في منظمات وحكومات في جميع أنحاء العالم. إن مثل هذه الأحداث تعرض للخطر مدى فعالية مواد الحماية المعروفة في أوساط المؤسسات والحكومات.

إن الربط بين مجال الحاسوب وبين التجهيزات العاملة في مجالات أخرى – على سبيل المثال المجسات- يجعل بالإمكان تحويل معطيات جغرافية، حرارية، ميكانيكية وغيرها من المجالات المادية إلى وحدة ذاكرة والعكس، ويمكننا باستخدام مؤثرات تحويل الأوامر ذات العلاقة بشبكة وحدة الذاكرة إلى عمليات في هذه المجالات. إن هذا الدمج يتيح الفرصة لشن الهجوم المحوسب، وإحداث تأثيرات في المجالات المادية بواسطة مهاجمة منظومات مرتبطة بمجال الحاسوب، مثل المنظومات المرتبطة بالحواسيب: Computer Embedded system .

إمكانية العودة بالزمن إلى الوراء:

تعتبر هذه الميزة بمثابة مقدرة على التخلص السريع من الهجوم في مجال الحاسوب بواسطة إعادة خطوات الحاسوب إلى الوراء – العودة بالزمن بالاستعانة بأجهزة دعم معينة، وكلما كانت هذه الأجهزة شاملة وأكثر تواصلا كلما أصبح بالإمكان العودة إلى الصورة الأصلية لوضع الحاسوب بشكل أدق. وعلى أية حال فإن التخلص من الهجوم على الحواسيب سيكون أسرع وأرخص مقارنة بالدمار المادي الذي يلحقه الهجوم التقليدي بالنيران. ومع ذلك فإن هجمات حاسوبية أخرى بصورة معينة يمكنها أن تلحق أضرارا مادية جسيمة لا يمكن إصلاحها. أما على صعيد المهاجم: فإلى جانب التفوق، فإن هذه الخاصية تتيح الفرصة له لإلحاق أضرار محدودة ومؤقتة ببنية المعتدى عليه لتمييزها عن الهجمات والدمار الذي يمكن للهجوم التقليدي أن يحدثه في هذه البنية، والتي تبدو أحيانا غير مرغوب فيها، وخصوصا حينما تكون هذه البنية مدنية.

وإضافة إلى العيب آنف الذكر الذي أشرنا إليه بالنسبة للمهاجم، فهناك أيضا مقدرة المعتدى عليه في التخلص سريعا من آثار الضربة بوضع العراقيل على طريق المهاجم وحماية نفسه من الوسائل التي سبق أن تعرض عبرها للهجوم، الأمر الذي يحول "أسلحة" الهجوم الحاسوبية إلى أسلحة ذات استخدام لمرة واحدة، مما يجعل من الصعب على المهاجم خلق أضرار تراكمية والمحافظة على تواصل الهجمات وقوتها. ولا شك أن هذا

التحدي هو تحد كبير للمهاجم الساعي للتوصل إلى إنجازات إستراتيجية عبر شن هجمات حاسوب متواصلة وواسعة النطاق. وبناء على هذه الصعوبات يعتقد بعض الباحثين أن احتمالات إلحاق الأضرار بالعدو أو تحقيق المهاجم إنجازات عبر الهجمات التي تشن على الحواسيب ضئيلة نسبيا أكثر مما يقدر الكثير من الباحثين والخبراء.

مقدرة سيطرة إنسانية عالية على مجال الحاسوب:

نظرا لأن مجال الحاسوب هو مجال مصطنع، وصناعة الإنسان فمن المتوقع أن يتمكن المدافع من السيطرة على المجال الذي خلقه، ومن المفروض أن يتوقع الشروط في المجالات الأخرى على عكس المجالات الأخرى التي تجد صعوبات في التنبؤ بالشروط التي ستسود مثل المناخ على سبيل المثال. كما أن بمقدوره تعطيل المجال أو تقليص استخدامه. ويمكننا أن نجد نماذج لمحاولات تقليص استخدام المجال في الصين، وفي الدول العربية وإيران. هذا إضافة إلى أن من الأسهل حماية وترميم شبكة منظمة ومرتبة أسرع من حماية وترميم شبكة غير منظمة. إن هذا المجال يتيح الفرصة للجانبين -المهاجم والمدافع- التدرب بسهولة كبيرة وتنفيذ عمليات مماثلة.

ورغم ما أوردناه أعلاه يمكننا أن نجد في مجال الحاسوب أحداثا مفاجئة، لم يتوقعها أولئك الذين بنوا هذا المجال، وهي نتاج للتفاعل بين أجهزة الحاسوب أو تفاعل الأخطاء الإنسانية – على غرار الأخطاء التي ترتكب في إعطاء الأوامر في الأسواق المالية. كما أن خصائص المجال تعزز مقدرة الخبراء على تنفيذ عمليات شريرة بواسطته.

مجال مدني عسكري مشترك:

ترتبط وسائل الاتصالات العسكرية في الكثير من الحالات بوسائل الاتصال المدنية، وبناء عليه فإن الدفاع عن البنى المدنية يعتبر حيوياً أيضا بالنسبة للبنى العسكرية. كما أن الجيوش تتمتع بقدرة على صعيد مجال الحاسوب يمكنها حماية البنى المدنية. إن الدمج بين المجالين في الدول الديمقراطية هو تحد قضائي

للمدافع إزاء التشريعات الحديثة الخاصة بحقوق المواطن، والتي تصعب عملية جمع المعلومات وتفعيل وحدات عسكرية في مجال الحاسوب المدني.

الاتصال واستغلال موارد الاتصالات والحاسوب الخاصة بجهات أخرى: تعتبر شبكات الاتصال الدولية بالنسبة للمهاجم وسيلة تمكنه من اجتياز الحدود والتحرك بسرعة نحو الأهداف المرتبطة بها، واستخدام موارد الاتصالات والحواسيب الخاصة بالخصم من أجل مهاجمة أجهزته. وفي نفس الوقت تتيح هذه الاتصالات للمدافع إمكانية الاستعانة بالدول الصديقة من أجل اكتشاف الهجوم وإحباطه قبل أن يصل إلى دولته.

علاقة تواكلية تبادلية بين مجال الحواسيب والمجالات المادية: يقيم مجال الحاسوب علاقة اتكالية ذات اتجاهين مع المجالات المادية: فمن ناحية يعزز النشاطات في هذه المجالات ومن الناحية الأخرى يتيح الفرصة لتوجيه الضربات على الأهداف في تلك المجالات بواسطته. إن توجيه ضربات تقليدية للبنى المادية، مثل منشآت الاتصالات ومحطات الطاقة يساهم في حرب التحكم الآلي .

قدرة تطوير كبيرة لأسلحة حرب التحكم الآلي بسرعة وبتكلفة ضئيلة جدا: منذ اللحظة التي يتم فيها تطوير "سلاح حاسوب" مثل "الديدان"، أو البرامج الدفاعية يصبح من السهل استنساخه بكميات كبيرة دون أية جهود أو تكلفة عالية، وذلك على عكس الأسلحة التقليدية، ولا شك أن هذه الخاصية تخدم كلا من المهاجم والمدافع.

استغلال الموارد عن بعد:

يتيح مجال الحاسوب الفرصة لاستخدام موارد الطاقة البشرية وموارد الحوسبة بصورة خاصة، وهو الأمر غير المتاح في المجال المادي. وعلى عكس ميدان القتال التقليدي والذي يطالب خلاله الجنود بالوصول إلى ميدان المعركة، فإن بمقدور الجنود وموارد الحاسوب العاملين في ميدان حرب التحكم الآلي التواجد في أماكن مختلفة ويخوضون الحرب بسرعة فائقة عبر تكنولوجيا المعلومات. ولا شك أن هذا الوضع يحسن قدرة استخدام قوات الاحتياط في مجال الحاسوب إلى حد كبير.

استبدال مستمر للوسائل:

إن التطوير التكنولوجي ونقاط الضعف التي يتم العثور عليها في المنظومات القائمة تحتاج إلى عمليات تغيير متواصلة لوسائل الدفاع. وكذلك الأمر بالنسبة للتطوير المتواصل للمقدرة الدفاعية وإغلاق الثغرات والذي يتطلب العمل دائما على تطوير وسائل الهجوم.

إن هذه المسألة تعتبر بمثابة نقص كبير بالنسبة للمدافع نظرا لأنه مضطر لاستبدال كميات أكبر من الوسائل التي مضى زمنها.

معيار بداية متدني:

تضع خصائص مجال الحاسوب قيودا قليلة على بناء القدرة الهجومية لحرب التحكم الآلي المعقولة مقابل بناء الجيوش الذي يقوم على قوات متحركة. ونورد فيما يلي شكلا مقارنا:

أ- التكنولوجيا: تتوفر كميات كبيرة من الوسائل التكنولوجية في السوق الحر، وبمقدور المهاجم أن يشتري منظومات دفاعية يستخدمها الخصم، وإنفاق مبالغ على تطوير مقدرته الهجومية حتى إحراز التفوق التكنولوجي.

ب- معلومات هجومية: هناك كم هائل من المعلومات الهجومية في السوق الحر، على سبيل المثال في أيدي قراصنة الإنترنت، وبأيدي شركات الأعمال التي تقوم بتوفير خدمات هجومية في مجال الحاسوب، وبشكل خاص لأغراض الفحص والتدريب على منظومات الدفاع لشركات ومنظمات.

ت- رأس المال المطلوب لتطوير قدرة هجومية متدني إلى حد كبير مقارنة برأس المال المطلوب لإقامة جيش تقليدي حديث.

بمقدور الدول أن تنشئ قوات حرب حاسوب ذات قدرة هجومية متقدمة بأسعار متدنية مقارنة بتلك المطلوبة من أجل بناء قوات عسكرية متقدمة. وبمقدور المنظمات والمجموعات هي أيضا التجهز وتفعيل أسلحة حاسوب. وبمقدورها أن تستأجر مدنيين وشركات خاصة لتعمل بدلا عنها. ومثلما قال نائب وزير الدفاع

الأمريكي وليام لين: "بمقدور عدة عشرات من المبرمجين المؤهلين أن يلحقوا أضرارا جسيمة". ورغم ذلك يجب أن نميز بين القدرة الهجومية التي يمكنها أن تلحق أضرارا آنية أو دائمة – مهما كان مدى قسوة هذه الأضرار- وبين إمكانية تنفيذ الهجوم الحاسوبي الواسع والمتواصل على الأهداف الإستراتيجية للعدو الذي يمتلك مقدرة دفاعية متطورة. ويخيل لي إن هجوما من النوع الثاني يتطلب مقدرة لا تملكها حتى الآن سوى دول ذات قدرة تكنولوجية عالية. إن وسائل الدفاع ضد الهجوم الحاسوبي متوفرة في السوق الحر، بيد أن الدفاع الحاسوبي الشامل يتطلب توفير ردود ناجعة لسلسلة كبيرة من أنواع التهديدات وهو الأمر الذي يتطلب توفير مبالغ كبيرة.

مجال الحاسوب: مصطلحات أمنية تقليدية ذات محتوى جديد:

يختلف مجال التحكم الآلي كثيراً في العديد من الأصعدة عن المجالات المادية، بما فيها في المجال الأمني. ولا شك أن هذا الاختلاف الكبير يتطلب أن نعيد النظر من جديد في فاعلية المصطلحات الإستراتيجية التقليدية وصب مفاهيم جديدة فيها. هناك العديد من المصطلحات في وثائق الجيش الأميركي التي تتعلق بمجال التحكم الآلي، ورغم ذلك يبدو أن المصطلحات الأولى التي خدمت ميادين القتال التقليدية تخدم ميادين القتال في حرب التحكم الآلي: الردع، الدفاع، الهجوم، سباق التسلح وغيره. ومن الجائز أن هذه المصطلحات ستبقى عاملة سنوات طويلة مع ملاءمتها مع المجال الجديد، ومن الجائز أن هذه المرحلة هي مرحلة انتقالية حتى بلورة مصطلحات جديدة لدى المؤسسات الأمنية.

البيئة الإستراتيجية:

تختلف البيئة الإستراتيجية للتحكم الآلي عن البيئة الإستراتيجية التقليدية والتي اعتادت إسرائيل عبرها تحديد دوائر العداء الجغرافية. والعلاقة بين مجال التحكم الآلي والجغرافي يتعلق بالانتشار الجغرافي لبنية الحاسوب والشبكات، الأمر الذي يمنح مصطلح الجغرافية معنى مختلفا في مجال التحكم الآلي. كما أن التعامل مع معيار الزمن في مجال التحكم الآلي مختلف عن التعامل العادي مع الزمن نظرا للسرعة التي تتحرك

بها وحدات الذاكرة في المجال الإلكترو- مغناطيسي. وبناء عليه يمكن لمجال التحكم الآلي أن يعزز قوة أعداء قدامى ويمكن أن ينضم إليهم أعداء ولاعبون جدد ومختلفون والذين وجدوا صعوبات بالغة في المشاركة في معارك سابقة سواء كان ذلك بسبب البعد أو الاختلافات الجغرافية.

كما أن مجال التحكم الآلي يخلق فرصاً أمنية جديدة ويتيح الفرصة للاستعانة بحلفاء بصورة مختلفة وفقا لمقدرتهم ومكانتهم في هذا المجال، ولهذا السبب ونظرا للأولوية التي ستمنحها دول مختلفة لتطوير قدرة تحكم آلي فمن الجائز أن تنشأ توازنات قوى جديدة بين الدول أو بين دول ومنظمات خارج الدول- منظمات إرهابية، مجموعات قراصنة حواسيب دولية أو فوضويين. وبناء عليه فإن مجال التحكم الآلي يخلق بيئة إستراتيجية متفردة ويوسع البيئة الإستراتيجية بصورة عامة.

ونلاحظ وجود ثلاثة مجالات عمل على صعيد العمليات الأمنية ضد الأعداء في البيئة الإستراتيجية للتحكم الآلي:

أ- اختراق منظومات الاتصالات المعادية من أجل التجسس. رغم أن هذا الاختراق لا يأتي في إطار حرب التحكم الآلي.

ب- حرب تحكم آلي لينة Soft Cyber Warfare نشاطات في مجال التحكم الآلي ترمي لتشويش عمل العدو، مثل الحرب النفسية، وعدم التسبب في التدمير بصورة مباشرة.

ت- حرب التحكم الآلي، والتي تتضمن نشاطات في مجال التحكم الآلي تشمل هجمات ترمي لإلحاق أضرار أو دمار بالعدو بصورة مباشرة، بما فيها أضرار لمنظومات الاتصالات والحاسوب أو أهداف في مجالات مادية عبر إلحاق الأضرار بالتجهيزات التي يسيطر عليها التحكم الآلي أو تفعيلها بصورة تلحق أضرارا.

إن الجهات المسؤولة عن مثل هذه العمليات في دول العالم هي جهات أمنية وعسكرية ومنظمات استخبارية، ورغم ذلك يشارك في الدفاع عن مجال التحكم الآلي جهات كثيرة في القطاعات المدنية ومن ضمنهم الوزارات الحكومية- مثل وزارة أمن الوطن في الولايات المتحدة، وشركات خاصة – شركات حماية، تكنولوجية واتصالات. إن خلق منظومات مشتركة ومركزية لجميع الجهات المشاركة في الدفاع والتوازن المشترك بين المدافعين وقوات الهجوم تشكل تحديّاًً مركزياً لصانعي إستراتيجيات التحكم الآلي على المستوى القومي.

التجسس وحرب التحكم الآلي اللينة:

التجسس:

إن عمليات التجسس هي عمليات اقتحام – وليست هجوم- شائعة الاستخدام في إطار المهام التي تقوم بها المؤسسات الأمنية في مجال التحكم الآلي. وهذه العمليات لا ترمي للمساس ولتشويش منظومات العدو، أو للتأثير عليها بصورة مباشرة. هناك تاريخ طويل لاستخدام مجال التحكم الآلي من أجل جمع المعلومات يرجع إلى بداية الحاسوب في الحياة العامة، ويمكننا أن نميز في هذا المجال بين ثلاثة أنواع من العمليات:

أ- جمع المعلومات الاستخبارية: حول إمكانية العدو ونواياه خلال حالات السلم والحرب من أجل تقدير الوضع، وبلورة الإستراتيجيات واتخاذ القرار وبناء القوة العسكرية المقاتلة.

ب- التجسس الصناعي: بما فيها سرقة أسرار تكنولوجية وأسرار عمل.

ت- التقاط معلومات تحكم آلي تتعلق بالعدو، مثل سرقة مخططات وبرامج ومعطيات بغية استخدامها دون إذن. إن هذه القضية تشذ عن مجال جمع المعلومات وهي قريبة أكثر من استخدام أسلحة غنائم أو سرقة ممتلكات. ويمكن القيام بسرقة ممتلكات التحكم الآلي عبر استنساخها ودون إخراجها من حوزة العدو.

من الجدير بالذكر أن الفعالية القائمة في القوة الاقتصادية والتكنولوجية تأثير كبير جدا على توازن القوى الإستراتيجية، فإن عمليات جمع المعلومات والممتلكات الخاصة بالتحكم الآلي والتكنولوجي والاقتصادي يمكنها أن تعكس تأثيرا هائلا على الأمن القومي للطرفين. إن بمقدور هذه المعلومات والممتلكات أن تحسن مقدرة التنافس للدولة التي تجمعها على الصعيد العالمي وتحسن مقدرتها على صعيد تقليص الفوارق في مجال الأبحاث والتطوير الأمني. كما أن الدولة التي تم اختراقها ستفقد تفوقها الإستراتيجي. إن الأمر يتعلق بمجال تتخطى فيه عملية جمع المعلومات الاحتياجات التقليدية لجمع المعلومات من أجل التعرف على العدو ومعرفة مقدرته ونواياه.

لقد أشارت صحيفة نيويورك تايمز إلى حادثة يمكننا اعتبارها كأول حادثة على صعيد التجسس في مجال التحكم الآلي. فقد نجحت روسيا في السبعينات في اختراق ARPANET -شبكة الاتصالات التابعة للوكالة الأميركية لمشروعات الأبحاث المتقدمة التي سبقت وجود الانترنت. وقد اتضح في إطار مشروع عسكري قامت الولايات المتحدة بتمويله في مركز الأبحاث الرقمية في جنيف، أن جهاز إرسال الشبكة موصول بموسكو، وأنه يمكن الروس من اختراق الولايات المتحدة عبر هذه الشبكة.

لقد طرح نائب وزير الدفاع الأميركي وليام لين نموذجا آخر لحادثة تجسس خطيرة على صعيد التحكم الآلي، فقد أفاد أن وكالة مخابرات أجنبية نجحت عام 2008 في اختراق منظومات حاسوب سرية في الولايات المتحدة باستخدام قرص يمكن فصله، وبصورة كنا نعتقد أنها مستحيلة. لقد كانت هذه العملية بمثابة تجسيد لمخاوف كانت تراودني، برنامج ذكي يعمل بصورة هادئة في منظوماتنا وينقل برامج عملية إلى أيدي الأعداء".

ومن الجائز أن هذه الأوصاف تتعلق بالاختراق المنسوب إلى الصين، والذي في إطاره سرقت مخططات الطائرة الحربية المستقبلية F-35 Lightning 2- التي كانت شركة لوكهيد مارتن تعكف على تطويرها،

بما فيها المنظومات الالكترونية للطائرة والتي تعتبر أحدث طائرة في العالم، والتي أنفقت الشركة على عملية تطويرها ثلاثمائة مليار دولار.

لقد وصف لين ظاهرة السرقات في مجال التحكم الآلي على النحو التالي: "لقد سرقت منظمات استخبارية في الجانب الأمني برامج عسكرية وبرامج أسلحة. أما على الصعيد التجاري فقد سرقت مخططات باهظة الثمن وممتلكات روحية من شركات أعمال وجامعات. حقا أن هذه الاعتداءات والهجمات ليست ذات تأثير درامي مثل الهجمات التقليدية، بيد أن تأثيرها على المدى البعيد مدمر نظرا لأنها تقلص التفوق الأميركي في مجال التكنولوجيا العسكرية وتمس بكفاءة المنافسة الأميركية أمام الاقتصاد العالمي.

حرب رسائل المعلومات:

حرب الرسائل الالكترونية هي حرب لينة تستخدم المعلومات بصورة مكثفة، وهي تعتبر بمثابة عامل مركزي في مجال الحرب النفسية، والتضليل، والدعاية، وكشف المعلومات التي يُعنى العدو بإخفائها. والهدف الأساس من هذه الحرب هو التأثير على أراء ومسلكية العدو ومؤيديه بصورة تتناسب وأهداف الجانب المبادر ودون المبادرة لاستخدام القوة العسكرية. وذلك على عكس عمليات التجسس. أما الجانب الآخر في هذه "العائلة" فهو جانب الإعلام الذي يرمي لتوفير معلومات وإبراز منطقية الأحداث لجماهير الدولة والأصدقاء، الأمر الذي يعتبر حيويا بالنسبة لمشروعية استخدام القوة العسكرية. لقد طرأت زيادة مضطردة منذ انتقال وسائل الإعلام إلى مرحلة الانترنت في سنوات التسعينات على استخدام مجال حرب التحكم الآلي في حرب رسائل المعلومات وأيضا في مجال الإعلام.

إن الفارق الأساسي بين حرب رسائل المعلومات في مجال حرب التحكم الآلي وبين هجوم حرب التحكم الآلي هو الجهة التي تتعرض بصورة مباشرة للهجوم. وبناء على هذا الوضع يبدو الاختلاف في الصورة التي يتم إعداد المعلومات بها: فحرب رسائل المعلومات تستخدم بصورة عامة المعلومات المنظمة والمعروضة بصورة

يمكن للمستخدم العادي فهمها – فالرسالة هي معلومة يمكن لبني البشر فهمها- في حين أن هجوم التحكم الآلي يجري على الصعيد المادي أو الرمزي وباللغة التي يفهمها خبراء البرمجة والالكترونيات.

وتعترف الولايات المتحدة بقوة مجال حرب رسائل المعلومات الهائل، وقد شنت في العراق حربا نفسية ضد القاعدة. ويعمل الأميركيون في الآونة الحالية لتوسيع إطار الحرب ضد الجهات الإسلامية المعادية في باكستان، أفغانستان وإيران وأنحاء الشرق الأوسط . كما شرع الأميركيون بحملة لتغيير الرأي العام السلبي تجاههم في العالم الإسلامي. ويمكننا أن نستدل على ذلك على سبيل المثال من الشهادة التي أدلى بها الجنرال ديفيد بتراوس قائد قوات الائتلاف الأميركي في أفغانستان أمام الكونجرس الأميركي في آذار 2011. وقد تحدث في شهادته عن الجهد المطلوب من أجل تعزيز النشاطات الاستخبارية الأميركية في الشبكات الاجتماعية من أجل التصدي للمعركة الأيديولوجية والدعاية الجارية ضد الولايات المتحدة والغرب. وفي إطار هذه الجهود يجري تطوير برامج تتيح الفرصة للتدخل سرا في الشبكات الاجتماعية. فعلى سبيل المثال حظيت شركة أميركية من كاليفورنيا بمناقصة للجيش الأميركي لتطوير خدمات إدارة موجهات تمكن مستخدم واحد من إدارة عشر شخصيات منتحلة في الانترنت، على أن تبنى كل شخصية بخلفية تاريخية مفصلة مع استخدام الخدمات التي يوفرها العالم من أجل خلق انطباع يفيد أن الردود تأتي من أماكن مختلفة من العالم. ويمكن البرنامج الأشخاص المنتحلين من التدخل في النقاشات باللغة العربية والفارسية ولغات أخرى تستخدم في باكستان وأفغانستان.

لقد تجهز سلاح الجو الأميركي بطائرات من طراز هركلوس 130C والمخصصة لتنفيذ مهام في أطار الحرب النفسية، مثل إمكانية التسلل إلى البث التليفزيوني والإذاعي للدول المعادية وبث رسائل ضد نظام تلك الدولة أو توجيه رسائل لمواطني تلك الدولة، والعمل كجهاز قادر على إنشاء شبكة تليفونات خلوية تمنح سكان الدولة خدمات تليفونية متحركة وإنترنت لاسلكي وإجراء الاتصالات معهم إذا حاول النظام قطع الاتصالات. أي أن بمقدور أجهزة هذه الطائرة مصادرة التحكم الآلي الالكترونية من أيدي النظام من أجل تحسين مصالح المهاجم.

وليس أدل على القوة الهائلة التي تتمتع بها حرب رسائل المعلومات من الثورات الناشبة في الشرق الأوسط بمساعدة مجال التحكم الآلي.

لقد نجح الشبان الذين يستخدمون رسائل المعلومات والتحكم الآلي في إحداث ثورة في الدول العربية على غرار ما حدث في مصر وتونس. إن الأمر يتعلق بحرب يعتبر التحكم الآلي فيها بمثابة واسطة مساعدة ومؤثرة، بيد أن أعداء النظام في هذه الحالة هم مواطنو الدولة وليس أعداء خارجيين.

هناك مجال آخر لحرب رسائل المعلومات وهو اكتشاف أسرار العدو بهدف إلحاق الأضرار به، واكتشاف نواياه ونشاطاته المحظورة،وتصريحاته المحرجة وما شابه. وتبرز في هذه الحالات نشاطات الأفراد والمنظمات السياسية ضد المؤسسات السياسية.

عقوبات تحكم آلي:

تعتبر العقوبات بمثابة حرب لينة، وليست سرية هدفها معاقبة منتهكي القواعد - بناء على رؤيا المعاقب- من أجل دفعه لتغيير تصرفاته وردعه عن تنفيذ أعماله مرة أخرى أو إضعافه توطئة لاستخدام وسائل ضغط أخرى. وهناك سلسلة واسعة من العقوبات بدءا من منعه من التعاون والكثير من الحقوق الأخرى من الدولة "الهدف" والعزل، وفرض الحصار على حدودها - على غرار الحصار الذي فرضه الائتلاف الأميركي على العراق على عهد صدام حسين. ومن الجدير بالذكر أن مجال التحكم الآلي جذاب بالنسبة للعقوبات، نظرا لسهولة العمليات التي يمكن القيام بها من أجل ذلك مثل حجب وسائل الإعلام مع الخارج وهو الأمر الذي يعتبر مؤثرا إلى حد كبير، ورغم ذلك فإن فرض عقوبات تحكم آلي فعالة تتطلب ائتلافا من الدول ذات العلاقة.

وبالإمكان فرض عقوبات تحكم آلي كجزء من مجموعة عقوبات على الدولة "الهدف" أو كجزء من بلورة قواعد لعبة في مجال التحكم الآلي. ويقول مايكل هيدن: إن الإدارة الأميركية فكرت في السابق القيام بعمليات ضد الدول التي تنطلق منها هجمات تحكم آلي على الولايات المتحدة بما فيها استخدام عمليات العزل الآلي، أو الرد التهديدي أو الذي يلحق أضرارا بتيار تدفق المعلومات عبر الانترنت لتلك الدولة.

حرب التحكم الآلي:

هجوم التحكم الآلي هو عملية حربيـة في مجـال الـتحكم الآلي ضـد العـدو مـن أجـل إلحـاق خسـائر بـه، والمساس بمقدرته على الأداء وإرغامه على العمل وفقا لرغبـات المهـاجم. والهجـوم عـبر الـتحكم الآلي بحـد ذاتـه غـير مؤهل لحسم الأمور أو إحراز إنجازات إستراتيجية تعادل احتلال المناطق بأيدي القوات البرية، بيد أنه مؤهل لإلحاق الأضرار بأهداف العدو الحيوية وبقدراته.

وقد تطرق قائد قيادة التحكم الآلي الأميركي خلال الشهادة التي أدلى بها في الكونجرس في نيسان 2010 إلى أنوع الأهداف المرشحة للهجوم في مجـال الـتحكم الآلي ومـن ضـمنها: منظومـات الـدفاع الجـوي، منظومـات حربيـة وأجهزة الرقابة والسيطرة العسكرية، البنى المدنية ومن ضمنها شبكات الكهرباء والهيئات والأجهـزة الماليـة، وأجهـزة الاتصال والمواصلات.

وبناء عليه يمكننا الافتراض أن الهجوم عبر التحكم الآلي يمكنه أن يكون عاملا من عوامل أية حـرب حديثـة في المستقبل إلى جانب العوامل البشرية الأخرى. إن الخصائص الخاصة بمجال التحكم الآلي تجعله مجالا جذابا للحرب حتى خلال فترات الهدنة ما بين الحروب التقليدية. ويمكن لهجمات التحكم الآلي أن تستخدم للأهداف التالية:

أ- وسيلة لممارسة ضغوط لتغيير سياسات العدو – على غرار الهجوم المنسـوب إلى روسـيا ضـد أستونيا- خلال مراحل الهدنة بين الحروب التقليدية.

ب- إحباط التهديدات الأمنية المتشكلة، على غرار الهجـوم الـذي شـنه فـيروس "ستاكسـنت" في إيران.

ت- بناء مقدرة هجومية كجزء من ميزان الردع.

ث- رد مضاد: مهاجمة المعتدي أو الدول التي انطلق منها عبر التحكم الآلي.

ورغم أن قضية الاعتداءات في مجال التحكم الآلي لم تصل إلى حد التنظيم في القانون الدولي، فإن الهجوم على هذا الصعيد قد يعتبر بمثابة إعلان حالة حرب، هذا في حين أن عمليات التجسس عبر التحكم الآلي التي لا تلحق أضرارا فورية ملموسة لا تعتبر كذلك.

إن الهجمات التي تشن في مجال التحكم الآلي تجري بصورة عامة على الصعيد الرمزي، بيد أن هناك اعتداءات وهجمات تتسم بخطورة بالغة. ويمكننا أن نميز بين نوعين من الهجمات: الأولى ترمي لتشويش أو إلحاق الأضرار في مجال التحكم الآلي للعدو – حواسيب، شبكات، قواعد معلومات وغيره- بصورة تمنعه من استخدام التحكم الآلي لمصلحته -على غرار الهجوم المنسوب إلى روسيا في أستونيا- ومهاجمة منشآت البنية التحتية والمعدات الحربية، مثل مهاجمة فيروس "ستاكسنت" للمنشآت النووية الإيرانية.

ويؤكد مسؤولون أميركيون رفيعو المستوى أن هناك ميزة للهجوم على الدفاع في مجال التحكم الآلي. ويقول نائب وزير الدفاع الأميركي وليام لين: إن التفوق الذي يتمتع به المهاجمون في حرب التحكم الآلي ناجم عن كون الانترنت بني كمجال مفتوح يضمن تدفق المعلومات وتلقي تكنولوجيا جديدة وفي نفس الوقت منح مجال الأمن في شبكة الانترنت أهمية ضئيلة. ولا شك أن هذه الاتجاهات أسهمت في تطوير الانترنت، بيد أنها أيضا تعطي المهاجم الأفضلية. ويمكننا أن نرى ذلك عبر المقارنة بين برامج الحماية من الفيروس والبرامج الهجومية. فبرامج الحماية من الفيروس الذكية تستخدم حوالي عشرة ملايين خط من الرموز، مقابل مليون خط قبل سنة، ورغم ذلك فإن البرامج الهجومية المؤلفة من 125 خطا من الرموز والتي لا يزيد طولها عما كانت عليه في السنة الماضية، مؤهلة لاختراق برامج الحماية من الفيروس.

ويميز وليام لين بين الهجمات التي تشن عبر التحكم الآلي والتي ترمي لتشويش محدد في الزمن والحجم – على غرار الهجوم الذي يشنه القراصنة، أو تخريب موقع عبر شن هجمات بسيطة للغاية،وبين الهجمات التي ترمي لإلحاق أضرار وتدمير البنى التحتية للتحكم الآلي للخصم. ورغم أن مثل هذه الهجمات لم تبد حتى الآن بصورة موسعة لكن الحقيقة هي أن تتضمن احتمالات مدمرة.

ويقول لين: رغم أن تهديد حرب الـتحكم الآلي لا تشـبه الحـرب التـي تهـدد الوجـود عـلى غـرار الحـروب النووية، إلا أن هناك خطوط تشابه فيما بينها. فمجال التحكم الآلي يوفر للأعداء إمكانيـة ووسـائل تقليديـة لتهديـد الولايات المتحدة، حقاً أن مثل هذه الهجمات لن تفضي إلى وقوع إصابات كبيرة، بيد أنها قد تـؤدي إلى شـل المجتمـع الأميركي بصورة مشابهة. أما على المدى البعيد فـيمكن للاخـتراق المتواصـل والمنهجـي مـن قبـل القراصـنة للجامعـات وشركات الأعمال أن يؤدي إلى سرقة المقتنيات الروحية الأميركية ويخلق تهديدا على تفوقها الاقتصادي العالمي.

ويميز الخبراء في مجال الاعتداءات عبر التحكم الآلي بين الأساليب الاختراقية التي تسـتخدم بـرامج شريـرة، وبين الأساليب غير الاختراقية بطبيعتها، مثل الهجمات التي تشن لوقف الخـدمات. DDoS . ويجـري إقحـام الـبرامج الشريرة Malware بأنواعها المختلفة في حواسيب الخصم سرا باسـتغلال نقـاط ضـعف في جهـاز الحمايـة. وبالإمكـان إتمام عملية الإقحام من الخارج عبر شبكات دولية وعالمية، أو من الداخل عبر عميل يعمل داخـل المنظمـة أو الجهـة محل الاختراق أو بالـدمج بـين الطـريقتين. وهنـاك أنـواع مـن الـبرامج الشريـرة، مثـل "دودة الحاسـوب، أو "حصـان طرواده"، والتي تتيح الفرصة للشخص الذي يقوم بعمليـة الاخـتراق بتنفيـذ العديـد مـن العمليـات والمهـام، كجمـع المعلومات أو شن الهجمات مثل: جمع المعلومات الاستخبارية المتراكمة في الحاسوب الذي يتعرض للهجوم، تشـويش عمل الحاسوب المعادي، محو ملفات فيه، السيطرة عليه والعمل عبره ضد حواسيب وأجهزة أخـرى مرتبطـة بـه. وفي الكثير من الحالات ما يتم توجيه البرامج الشريرة بحيث تنتشر إلى حواسيب أخرى قـد تكـون بحـوزة العـدو وأحيانـا بصورة غير مراقبة. وبمقدور بعض البرامج أن "تستقر" في حواسيب الخصم حتى يصدر إليها الأمر بالعمل.

إن الهجـمات التـي ترمـي إلى "منـع الاسـتخدام" DDoS - Distributed Denial of Service ترمـي لتشـويش مجـال الـتحكم الآلي للخصـم. وفي مثـل حـالات الهجـوم المـذكورة يـتم غمـر المواقـع التـي تتعـرض للهجـوم بعـدد كبـير جـدا مـن التوجهـات في آن واحـد إلى الدرجـة التـي لا تمكنهـا مـن الصـمود أمـام هـذه

التوجهات وتنهار. ويتم خلال هذه الهجمات استخدام الفوارق التقنية – استخدام مواقع لا يبدو لها صلة مع الجهة المهاجمة، واستخدام قراصنة الكمبيوتر من أجل الحيلولة دون قيام أية جهة بتجريمها. ويقول وليام لين: إن الهجمات الرامية لمنع الاستخدام والرامية لتشويش وتخريب منظومات المعلومات كانت حتى الآن قصيرة المدى، وذات معايير ضيقة وغير ذكية، بيد أن بمقدور الأعداء ذوي المقدرة العالية في المستقبل أن يبنوا مقدرة لشل شبكات على نطاق واسع، ولفترات زمنية أطول. إن التأثير الفني لمثل هذه الهجمات يمكن تصحيحه، بيد أنه من المستحيل تصحيح الأضرار الاقتصادية التي ألحقها الهجوم وكذلك فقدان الثقة بالشبكة. وأشار لين إلى أن الهجمات الرامية لمنع الاستخدام وجهت ضد شركات تجارية.

ويقول مايكل هيدن أن استخدام الهجمات الرامية لمنع الاستخدام كان أحد الإمكانيات التي درستها الإدارة الأميركية من أجل العمل ضد الدول التي تنطلق منها الاعتداءات على الولايات المتحدة نظرا لأن مثل هذه الاعتداءات محظورة بناء على ميثاق جنيف.

الردع:

يعترف الجميع بضعف هذا المصطلح التقليدي فيما يتعلق بمجال حرب السيطرة الآلية، نظرا لأنه يتعذر معرفة المسؤول عن الاعتداءات في جميع الحالات، خصوصا وأن بمقدور المهاجم استخدام بنى طرف ثالث. أضف إلى ذلك أن إحراز الردع يتطلب توفير مقدرة متنوعة، بيد أن اكتشاف هذه المقدرة يجعلها غير مجدية. وقد أدلى قائد قيادة التحكم الآلي الأميركي الجنرال ألكسندر بشهادته أمام الكونجرس الأميركي في نيسان **2010**، وقال فيها: إن الولايات المتحدة لم تبلور بعد نظرية ردع في مجال التحكم الآلي نظرا لصعوبة بلورة مثل هذه النظرية. إن أفضل طرق الردع تتمثل في تعزيز وسائل الحماية في شبكتنا.

ورغم ما أوردناه أعلاه، بالإمكان القيام بعمليات ردع في مجال التحكم الآلي، مثل تحذير الدول المعتدية – على غرار التحذيرات التي أطلقتها وزيرة الخارجية الأميركية هيلاري كلينتون تجاه الصين – القيام

بعمليات هجومية محدودة ضد الأعداء من أجل تجسيد مقدرة الرد ولو كان الثمن كشف بعض جوانب المقدرة التي نتمتع بها. ورغم صعوبة تنفيذ الردع، فإن من الجائز قيام توازن ردع بين الدول في مجال التحكم الآلي.

جدول 2: أنواع الاعتداءات في مجال التحكم الآلي:

الاعتداء	صورته
1- تشويش مقدرة الحوسبة والاتصالات	هجمات لا تغير صورة الحوسبة، بيد أنها تخلق عبئا مصطنعا على الشبكة، مما يتسبب في شلل وتشويش عملي لفترات زمنية معينة، مثل الهجمات الخاصة بمنع الخدمة DDoS
2- إلحاق أضرار بشبكة اتصالات وحوسبة الخصم.	هجمات تلحق أضرارا ودمارا في الاتصالات والحوسبة. وهذه الهجمات تغير مقدرة عمل الاتصالات والحوسبة أو قواعد البيانات، وتمنع الخصم من استغلال مجال التحكم الآلي لمصلحته.
3- استخدام مجال التحكم الآلي للخصم من أجل المساس بالأجهزة المربوطة بمجال التحكم الآلي أو إلحاق أضرار ودمار عبرها.	هجمات ليس من الضروري أن تغير إنتاج أجهزة الاتصالات والحوسبة نظرا لحاجتها إلى مجال التحكم الآلي من أجل شن هجوم على تجهيزات محوسبة – بنى حيوية، معدات حربية.

الحماية في مجال التحكم الآلي:

يثير تطور مجال التحكم الآلي - بوصفه مجالا حيويا لعمل الدول- لدى الدول قلقا تجاه ضرورة حمايته والحيلولة دون المساس بأية مجالات أخرى باستخدامه. وكلما استغلت دولة هذا المجال لمصلحتها، فسوف تكون أكثر عرضة للإصابة باستخدامه ضدها وضد مؤسساتها ذات الصلة به. وهذا الوضع ينطبق على

المنظمات والجهات الأمنية، فكلما ازداد اعتماد الجيوش والجهات الأمنية على مجال التحكم الآلي كلما ازداد اتكالها على وظائفه وكلما أصبحت عرضة أكثر للأضرار في هذا المجال والمجالات المرتبطة به.

إن هشاشة مجال التحكم الآلي على صعيد الحماية ناجمة من اعتماده على المجال الالكترو- مغناطيسي وبناه. إن حماية مجال التحكم الآلي يقوم على مواجهة عمليات اختراق شتى، بدءا من عمليات الاختراق لجمع المعلومات وانتهاء بهجمات التحكم الآلي. أما الأعداء الذين يتوجب على الجهاز الدفاعي أن يواجههم فهم على النحو التالي: الدول المعادية، المنظمات الإرهابية، الأشخاص العاملين في الداخل والذين يقومون بعمليات تخريبية، المجرمون على اختلاف أنواعهم، مجموعات القراصنة التي تعمل بحوافز أيديولوجية وغيرهم، والحوادث العارضة.

ورغم التصنيف الواسع آنف الذكر والذي يبدي مجال التحكم الآلي هو مجال بلا حدود، يجب أن نميز بين مجال التحكم الآلي العالمي وبين مجال التحكم الآلي للدولة والذي يعني: الحواسيب، المنظومات الآلية والشبكات، البرامج، المعلومات المحوسبة، المحتوى، معطيات نقل ورقابة، والمستخدمين لكل تلك الأشياء في الدولة وسكانها.

إن الحماية في مجال التحكم الآلي هي بمثابة تحد من نوع جديد، خصوصا إزاء مقدرة العدو في تنفيذ هجمات بسرعة البرق وصعوبة اكتشاف المعتدي. وقد أوضح قائد قيادة التحكم الآلي الأميركي الجنرال ألكسندر الوضع قائلا: عندما يتم اكتشاف عملية الاختراق للتحكم الآلي فليس بمقدور المدافع التأكد بصورة قاطعة من هدف هذا الاختراق، وبناء عليه فإن التمييز بين التجسس وبين محاولات الهجوم في مجال التحكم الآلي يكون صعبا للغاية في المرحلة الأولى على الأقل. إن التمييز بين عملية التجسس والاعتداءات هام على صعيد الرد المضاد، فالدول تشن الحروب إذا تعرضت لاعتداءات لكنها لا تشن حروبا في أعقاب تعرضها لعمليات تجسس نظرا لأن التجسس لا يعتبر بمثابة صورة من صور الحرب. ويمكننا القول: يكفي وجود ثغرة صغيرة أو خلية ضعيفة واحدة – سواء كانت إنسانية أو تكنولوجية- لإفشال عملية الحماية. إن مجال التحكم الآلي يعزز قدرة

الجهات المعادية في استغلال الثغرات في جهاز الدفاع لمصلحتها، وأجهزة الحماية هي في الكثير من الحالات عاجزة في مواجهة عمليات الاختراق التي يقوم بها أشخاص من داخل المنظومات وممن لديهم إذن بالعمل داخلها.

لقد وصفت وثائق الجيش الأميركي عام 2010 مصطلح الحماية في مجال التحكم الآلي على المستوى العملي، وبناء على هذه الوثائق فإن حماية التحكم الآلي هي بمثابة مجموعة من العمليات التي تتضمن حماية لشبكات الحاسوب وحماية لبنى هامة تصل إلى حد شن حرب واسعة والتي يمكن عبرها الرد في صورة هجوم مضاد أو هجوم وقائي. هذا وتتخذ في إطار حرب التحكم الآلي خطوات متنوعة بغية الحيلولة دون وقوع أضرار وتقليص حدة المخاطر والأضرار لبنى الاتصالات والحوسبة الحيوية. ومن ضمن هذه العمليات: الدعم لعزل منظومات معلومات وبيانات معينة، التفرقة بين المنظومات، نشر منظومات حماية معلومات تقليدية على عدة طبقات، حماية مادية لمنظومات المعلومات، وإجراءات أمنية لحماية المعلومات صلبة ومتغيرة.

إن نظرية الحماية الفعالة – والتي تعتبر أحد المركبات البارزة لإستراتيجية الحماية الشاملة في مجال التحكم الآلي في وزارة الدفاع الأميركية - هي بمثابة رد جزئي لتحديات سرعة هجوم التحكم الآلي. وتقوم هذه النظرية على إمكانيات استخبارية متطورة لاكتشاف وتشخيص أية نشاطات في الشبكة، وعلى أجهزة حماية آلية لاكتشاف الهجوم والرد الأوتوماتيكي دون التدخل البشري، وعلى مقدرة الرد الوقائي.

وبناء على ما أوردناه أعلاه، فإن من الواضح أن مصطلح حماية المعلومات والذي يُعنى بالحفاظ على المعلومات من السرقة والتخريب والأخطار لا يمكنه أن يسد جميع الثغرات في عملية الحماية لمجال التحكم الآلي نفسه والأجهزة المرتبطة به، مثل البنى الحساسة ومنظومات القتال. إن أنواع العمليات التي تعتبر مدمرة للغاية مثل استخدام مجال التحكم الآلي لإلحاق الأضرار- هذا وبالإمكان القيام بنفس العمليات دون إلحاق أضرار بمقدرة الحوسبة.

تحذيرات استخبارية:

استخدام هذا المصطلح لا يتطلب تنسيقا كبيرا في مجال التحكم الآلي بالنسبة للتحـذيرات الرئيسـة القائمـة على تحليل النوايا والتوجهات الإستراتيجية، وأساليب العمل والوسائل المتوفرة لدى العدو. بيد أن الأمر يختلف حينما يتعلق بتحذيرات تنفيذية وتكتيكية والتي تتطلب التطرق لتفاصيل الهجوم وتوقيتـه. وبالإمكـان الإعـداد للهجـوم في مجال التحكم الآلي بصورة سرية. وفي الكثير من الحالات يصعب معرفة أن الهجوم قد بدأ قبـل أن نـرى نتائجـه، بـل وفي الكثير من الحالات لا يتم اكتشاف تلك النتائج أبدا، وربما تعتبر تلك النتائج كعطب ما. إن السـؤال الـذي يطـرح نفسه هو: ما هو هدف التحذير في واقـع تجـري فيـه عمليـة الهجـوم بسرعـة الـبرق، ومـا هـي الخطـوات الدفاعيـة التنفيذية التي يمكنها أن تستفيد من هذا التحذير؟ إن نزوع الجيش الأميركي لبنـاء مقدرتـه الدفاعيـة والحمايـة عـلى منظومات الرد الآلي والتي ترد بصورة أوتوماتيكية حال اكتشافها للهجـوم يشـير إلى أن هنـاك حـالات يسـتحيل فيهـا الاعتماد على التحذيرات التكتيكية التقليدية – على غرار التحذيرات التـي يقـدمها المراقبـون الميـدانيون في الحـروب البرية حول تقدم قوات العدو.

الدمج بين القوات:

إن الدمج بين القوات المختلفة في الحرب يتيح الفرصة للحصول على مقدرة قتالية عاليـة. إن طـابع مجـال التحكم الآلي يتلاءم جيدا مع المثل القائل: "الصورة الكاملة أكبر من جميع أجزائها". ويمكـن لهجـوم الـتحكم الآلي أن يدمج مع الحرب الحركية، والحرب الالكترونية وحرب تسليم المعلومات. وفي حالات معينة تكون حرب الـتحكم الآلي بمثابة اتجاه رئيسي على أن تقوم مركبات وعوامل القوة الأخرى بتقديم المساعدة لهـا، وفي بعـض الأحيـان قـد يكـون العكس.

تعاون داخل الدول ومع الدول الأخرى:

إن التعاون في مجال حرب التحكم الآلي هو مسألة مركزية على صعيد الدفاع نظرا لأن هذا المجال يتجـاوز حدود الدول إلى العالم كله. ويمكننا أن نشير إلى نوعين أساسيين من هذا التعاون:

تعاون داخل الدولة:

إن التعاون في مجال حرب التحكم الآلي يعتبر بمثابة عامل أساسي في مجال الدفاع والحماية. وعلى عكس مجال الهجوم التقليدي الذي يمسك الجيش بزمامه، فإن بناء منظومة دفاع فعالة وقومية يتطلب تعاونا عميقا بين القطاع المدني والجيش. ونظرا لصعوبة الفصل بين البنى التحتية للتحكم الآلي المدنية والعسكرية، ونظرا لوجود قسم كبير من مقدرة التحكم الآلي في الدولة في أيدي مدنيين، فإن الأمر يحتاج إلى تعاون متعدد المجالات: تعاون داخل القطاع العام بين الوسطين المدني والأمني، وتعاون على محور آخر بين القطاع العام والخاص - شركات تكنولوجية متميزة، شركات اتصالات، شركات حماية، شركات بنى تحتية هامة وغيره.

إن التعاون مع الدول الأجنبية هو عامل هام على صعيد مواجهة التهديدات الجديدة نظرا للطابع الدولي والعالمي لمجال التحكم الآلي. وعلى سبيل المثال يمكننا باستخدام شبكات مشتركة وتعاون استخباري تحسين مقدرة الإنذار، والمتابعة المستمرة واكتشاف مسار الاعتداءات والرد عليها.

الجدول الثالث:

العمليات	أهداف وخصائص	نماذج لأضرار محتملة	نماذج لأضرار جسيمة
1-التجسس أ- جمع المعلومات	أ- الحصول على معلومات من أجل اتخاذ القرارات وتنفيذها، والتفوق في المعلومات على الخصم - ليست حرب تحكم آلي. ب- خصائص: عمليات سرية وخصوصا على الصعيد الرمزي،وهي ليست موجهة للتأثير على صورة الاتصالات والحوسبة أو على	اكتشاف أسرار تكتيكية أو تنفيذية موضعية لدى العدو	كشف أسرار إستراتيجية مما يضيع المفاجأة خلال الحرب، والتفوق الاستخباري على العدو

	قواعد المعلومات أو المستخدم. ج- لا يعتبر خطوة حربية		
ب- سرقة ممتلكات روحية وممتلكات تحكم آلي	أ- عمليات جمع معلومات للتفوق التكنولوجي العسكري والعملي – حرب تحكم الكتروني لينة. ب- خصائص: على غرار جمع المعلومات	فقدان ممتلكات روحية وممتلكات تحكم آلي معينة	فقدان التفوق التكنولوجي العسكري والعملي، إلحاق أضرار بالقدرة على المنافسة
2- حرب رسائل المعلومات (حرب نفسية، دعاية، كشف أسرار)	أ- استخدام رسائل المعلومات العلنية أو الخفية من أجل إحداث تغيير في مسلكية العدو أو الجهات المؤثرة عليه –حرب تحكم آلي لينة. ب- خصائص: استخدام واسع للمعلومات تجاه مستخدمي مجال التحكم الآلي. لا يرمي للمساس بالنشاط الوظيفي لمنظومات الاتصالات والحوسبة للعدو.	كشف أسرار تلحق أضرارا قصيرة الأمد بالمخططات التنفيذية، أضرار محدودة للإعلام	ضحية لخدعة إستراتيجية – فقدان المفاجأة في الحرب- التفوق الاستخباري على العدو.
3- عقوبات تحكم آلي	أ- عزل آلي للخصم من أجل إحداث التغيير في مسلكيته- حرب تحكم آلي لينة. ب- خصائص: وقف العلاقات في مجال الخدمات والتجارة في الحواسيب ووسائل الاتصالات	تعطيل وتشويش نشاطات التحكم الآلي	إسكات واسع ولزمن طويل لمجال التحكم الآلي

4- هجوم تحكم آلي أ-هجوم تحكم آلي لمجال التحكم الآلي	أ- مهاجمة أجهزة الاتصالات والحوسبة التي بحوزة العدو بغية المساس بنشاطاته – حرب تحكم آلي. ب- خصائص: عمليات فعالة وخصوصا على الصعيد الرمزي. ج- يمكن اعتبارها بمثابة إعلان حرب	أضرار محدودة لقواعد المعطيات وتشويش مؤقت لمجال التحكم الآلي	إسكات واسع لمجال التحكم الآلي فترة طويلة وفقدان قواعد معطيات حيوية بصورة واسعة
ب- هجوم تحكم آلي لتجهيزات مربوطة بمجال التحكم الآلي	مثلما أشرنا أعلاه، بيد أن الهجوم يخرج من حدود التحكم الآلي ويؤثر بصورة مباشرة على عمل أجهزة ومنظومات خارج هذا المجال.	المساس بعمل منشآت معدودة، وإمكانية الخروج منها بسرعة	إلحاق أضرار جسيمة بالبنى التحتية، والمقدرة العسكرية، أضرار جسيمة في الممتلكات وربما في الأرواح.

الفصل الثاني

حالات هجوم وعوامل

كابحة في مجال التحكم الآلي

- أول حادثة اعتداء عبر التحكم الآلي تنسب إلى وكالة المخابرات المركزية الأميركية التي قامت بزرع برنامج شرير لجهاز رقابة محوسب من إنتاج الولايات المتحدة.

- في عام 2008 تعرضت جورجيا لاعتداء تحكم آلي نسب لروسيا حيث تم استخدام أسلوب حجب الخدمة وقد أوقع الاعتداء أضرارا بالكثير من خدمات الانترنت العامة في الدولة وعطل مواقع حكومية.

- الاعتداء الذي شنته دودة "ستاكسنت" على إيران يعتبر بمثابة عهد جديد في مجال حرب التحكم الآلي.

- شن هجوم تحكم آلي يرتبط بمشاكل لا يستهان بها: فهناك ضبابية حول النتائج التي يمكن أن تسفر عن هذا الهجوم وهناك أخطار لا يستهان بها كما أن استخدام هذا النوع من الحرب يتطلب توفر مبررات وشروط سياسية.

إثر تعرفنا على طابع ميدان حرب التحكم الآلي ومصطلحاته ، سنستعرض باختصار تاريخ الاعتداءات المنسوبة إلى دول في هذا المجال. ومن الجدير بالذكر أن هذه العجالة لا تتضمن عمليات الاختراق من أجل التجسس، الحرب النفسية والجريمة. ويتضح أن قائمة أحداث الاعتداءات المنسوبة إلى دول قصيرة وتفتقر إلى المعلومات. ورغم أن الدول الغربية تتوقع عمليات إرهاب تحكم آلي، إلا أنه لا تتوفر حتى الآن أية معلومات حول قيام منظمة إرهابية بتنفيذ عملية إرهابية واسعة.

إن التقديرات التي تنشر في الجرائد المختلفة بشأن تشخيص الدولة التي تقف وراء هذا الاعتداء أو ذاك لا ترتكز على أدلة قوية بل على تقديرات الخبراء القائمة على تحليل المبررات والأسباب، وحجم العملية ومدى ذكائها وما شابه، بيد أن أية دولة لم تأخذ على عاتقها حتى الآن مسؤولية أي اعتداء تحكم آلي.

اعتداءات بارزة في مجال التحكم الآلي:

تنسب أول حادثة اعتداء عبر التحكم الآلي إلى وكالة المخابرات المركزية الأميركية التي قامت بزرع برنامج شرير لجهاز رقابة محوسب من إنتاج الولايات المتحدة والذي سبق أن قام الروس بسرقته ونقله من كندا إلى الاتحاد السوفييتي، ثم قاموا بتركيبه في أنبوب الغاز السيبيري في تموز 1982. وفي أعقاب تركيبها في الأنبوب وقع انفجار بسبب البرنامج "الشرير"، وقد وصف الانفجار بأنه أقوى انفجار غير نووي تتم مراقبته من الفضاء. وبناء على ما نشر كان هدف العملية الحد من عمليات سرقة التكنولوجيا والممتلكات الروحية من قبل عملاء الاتحاد السوفييتي. ويمكننا اعتبار هذه العملية بمثابة البشائر الأولى لحرب التحكم الآلي.

إن أول الاعتداءات الكبيرة في الشبكات الحديثة منسوبة إلى روسيا. ففي عام 2007 تعرضت مواقع انترنت حكومية كثيرة للاعتداءات في أستونيا – تم تعطيل المواقع لمدة يومين. وقد استخدم في الهجوم أسلوب حجب الخدمة DDoS . لقد كانت هذه العملية بالنسبة لأستونيا – التي تعتبر من أكثر الدول تقدما على صعيد استخدام الحاسوب والإنترنت- ضربة موجعة على صعيد مقدرة السلطة في السيطرة على الأوضاع.

لقد اكتشف الأستونيون أن الإكثار من استخدام الحاسوب هو بمثابة نقطة ضعف إزاء الهجوم الذي تعرضوا له في مجال التحكم الآلي. لقد شن الروس هجومهم على أستونيا بسبب قيام الأستونيين بنقل تمثال قتلى الجيش الأحمر خلال الحرب العالمية الثانية من وسط العاصمة إلى ضواحيها. وفي أعقاب هذا الاعتداء وقع حلف الناتو على اتفاقية تعاون مع أستونيا ينص على تقديمه المساعدة لها إذا تعرضت لأية اعتداءات مرة أخرى. لقد عزز الاعتداء معرفة دول الحلف بتهديدات حرب التحكم الآلي من قبل الدول المعادية، ورفع مستوى تلك الحرب إلى المستوى العالمي إلى الدرجة التي أصبح فيه الاعتداء على استونيا بمثابة نقطة تحول في ذاكرة الدول بالنسبة لحرب التحكم الآلي.

وفي عام 2008 تعرضت جورجيا لاعتداء تحكم آلي، وقد نسب هذا الاعتداء أيضا لروسيا. وبنفس الطريقة تم استخدام أسلوب حجب الخدمة. وقد أوقع الاعتداء أضرارا بالكثير من خدمات الانترنت العامة في الدولة وعطل مواقع حكومية. وعلى عكس الاعتداء على أستونيا، فإن الاعتداء الآلي على جورجيا لم يتوقف عند هذا الحد، بل سبق الحرب البرية التي شنها الروس عليها، ويبدو أن هدف هذا الاعتداء المساس بالعلاقة القائمة بين الحكومة والمواطنين. يمكننا اعتبار هذه الحالة بمثابة نموذج تكون فيه حرب التحكم الآلي مجرد وسيلة مساعدة للجهد الحربي التقليدي العام.

أما النماذج الأخرى للاعتداءات التي شملت حجب الخدمة أو اختراق مواقع الانترنت فهي على النحو التالي:

أ- الاعتداءات المنسوبة إلى كوريا الشمالية. ففي تموز 2009 تعرضت مواقع أميركية ومن ضمنها مواقع مؤسسات أميركية – مثل المباحث الفدرالية ووكالة المخابرات العامة ومؤسسة الفضاء ناسا- ومواقع مدنية – بنوك، ووسائل اتصالات ووسائل تجارية- لاعتداءات تحكم آلي. وفي نفس الوقت تعرضت منشآت ومؤسسات في كوريا الجنوبية لاعتداءات مماثلة، دون أن يتم اكتشاف أو معرفة الجهة التي تقف خلف هذه الاعتداءات. وعلى ما يبدو كانت هذه الاعتداءات هي رد فعل كوري شمالي على العقوبات التي فرضت عليها في تلك الآونة.

ب- في تشرين الثاني 2010 جرت معارك ثنائية في مجال التحكم الآلي بين قراصنة من الهند وباكستان، تمثلت في اعتداءات متبادلة على مواقع الانترنت الحكومية في الدولتين. وقد تعرض 270 موقع انترنت في الهند ردا على الاعتداء على 40 موقعا في باكستان.

ج- تعرضت إسرائيل لاعتداءات قراصنة من حزب الله، تركيا، شمال أفريقيا، وفلسطين وغيرها على مواقع رسمية وتجارية مثل موقع بنك إسرائيل، بنوك تجارية، موقع بلدية تل أبيب وغيره. وقد ازدادت وتيرة هذه الاعتداءات خلال الأحداث الأمنية مثل الحرب اللبنانية الثانية، عملية الرصاص المصبوب والتصدي لقوافل المساعدات إلى قطاع غزة، بيد أن أضرار تلك الاعتداءات كانت ضئيلة.

ويمكننا القول أن الاعتداء الذي شنته دودة "ستاكسنت" على إيران يعتبر بمثابة عهد جديد في مجال حرب التحكم الآلي. فقد علم في أيلول 2010 أن منشآت إيران النووية تعرضت لهجمات وأصيبت "بدودة ستاكسنت" والتي أدخلت إلى الشبكات في صيف 2009 . لقد أعربت شركة الحماية العالمية "سيمتكس" -والتي نشرت تقريرا كاملا حول هذا الاعتداء- عن اعتقادها بأنه تم ملاءمة الدودة لإلحاق الضرر بمحولات ذبذبات معينة والتي يجري تركيبها على أجهزة الطرد المركزية المخصصة لإخصاب اليورانيوم في إيران.

لقد اعترف الرئيس الإيراني محمود أحمدي نجاد بالاعتداء، بيد أنه حاول التقليل من شأنه، فقال: "لقد نجحوا في إلحاق الأذى بعدد محدود من أجهزة الطرد المركزي بواسطة برنامج تم تركيبه في القطع الالكترونية. ولحسن الطالع تمكن خبراؤنا من معالجة الأمر، وهم لا يستطيعون بعد ذلك العودة لنفس الفعلة". وفي أعقاب اكتشاف الاعتداء أصدرت شركة "سيمنس" برنامج لاكتشاف وإزالة الدودة،وشكل الإيرانيون طاقما لإزالتها. ومن الجدير بالذكر أنه وفي هذه الحالة أيضا لا توجد أية أدلة على الجهة التي تبنت الاعتداء. بيد أنه وبناء على أهداف الاعتداء ومستوى الذكاء المتميز الذي استخدم فيه، فإن وسائل الإعلام تشير إلى إسرائيل والولايات المتحدة، كما أن إيران اتهمت الدولتين بذلك.

لقد أثار هذا الاعتداء جدلا عالميا حول الحرب في مجال التحكم الآلي،حيث تعتبر شركات الحماية في مجال التحكم الآلي الاعتداء الذي قامت به دودة "ستاكسنت" بمثابة عهد جديد، وهنا اتفاق في الآراء على أن الاعتداء يمكنه أن يفضي إلى قفزة نوعية سواء كان ذلك على صعيد الحماية أو تطوير أسلحة الهجوم.

ونورد فيما يلي المغزى الذي ينسبه الخبراء الدوليون للهجوم:

أ- الاعتداءات التي تقوم بها دودة "ستاكسنت" مختلفة عن الاعتداءات السابقة، نظرا لأن الاعتداء تم بوسيلة ذكية ذكاء مفرطا يتمحور اعتداؤها حول هدف أمني محدد، وذلك على عكس الاعتداءات السابقة المنسوبة بشكل خاص إلى روسيا والتي استخدمت فيها وسائل بدائية وعلى جبهة واسعة.

ب- يعتبر الاعتداء بمثابة اعتداء أول من نوعه في عهد التحكم الآلي والذي تتسلل فيه هذه العمليات إلى المجال المادي المرتبط بالتحكم الآلي. أي أن الاعتداء يجسد فكرة الهجوم على مناحي خارج مجال التحكم الآلي باستخدام التحكم الآلي نفسه. وقد أشارت صحيفة "نيويورك تايمز" إلى أن هذه هي المرة الأولى التي ينتقل فيها برنامج حاسوب شرير من حاسوب إلى منظومة مهنية محددة تعمل في مجال الرقابة على التجهيزات الصناعية والموجودة في أجهزة مثل: شبكات الكهرباء، أجهزة الإنتاج في المصانع، أنابيب الغاز، السدود ومحطات الطاقة. لقد تمحورت الاعتداءات قبل ذلك في مجال التحكم الآلي حول مواقع الانترنت، وشبكات الشركات والشبكات العسكرية فقط.

ج- الحادثة تجسد احتمالية الأضرار الكبيرة التي يمكن للاعتداءات عبر التحكم الآلي واسعة النطاق والقائمة على وسائل ذكية من هذا النوع أن تلحقها. لقد وصفت إحدى المقالات التحليلية هذه البرامج الشريرة من نوع ستاكسنت باسم "Worms of mass destruction" وأشارت إلى أنها تشكل تهديدا حقيقيا على غرار الاعتداء الذي وقع عام 1999 تحت اسم "باج 2000" ولم يتحقق. وقد أفاد ممثل روسيا في حلف الناتو أن دودة "ستاكسنت" كان بمقدورها أن تتسبب في كارثة على غرار كارثة مفاعل "تشرنوبل".

د- من المحتمل أن تسقط الدودة المذكورة أو سلاح من نوعها في أيدي جهات قد تقوم باستخدامها مرة أخرى. وقد أشارت صحيفة "نيويورك تايمز" إلى أنه وفي أعقاب الحادثة ازدادت المخاوف في الولايات المتحدة من أن الحواسيب الأميركية معرضة للإصابة بأسلحة مماثلة. كما ثارت مخاوف من إمكانية أن تقع الدودة في أيدي جهات تخريبية أو منظمات إجرامية.

هـ- مخاوف من تسلل الدودة إلى دول أخرى. وقد أفادت شركة حماية سبق أن اكتشفت الدودة أنها تسللت إلى مائة ألف حاسوب، منها 60% في إيران والبقية في أندونيسيا والهند.

إن هذه الصورة تعكس أحداثا مركزية معروفة وتم نشرها، ومن الجائز أن هناك العديد من الاعتداءات والهجمات التي شنت في أنحاء العالم عبر التحكم الآلي ولم يتم اكتشافها حتى الآن، أو اعتبرت عطبا ما، أو لم يتم الإعلان عنها. ومن الجائز أيضا أن دولا مختلفة زرعت مقدرة هجومية في صورة حصان طروادة، أو زرعت برامج يمكن تشغيلها حين الحاجة.

عوامل أخرى أبرزت مسألة حرب التحكم الآلي:

رغم التاريخ الشحيح القصير جدا لحرب التحكم الآلي، إلا أن هناك على ما يبدو معرفة عميقة بمدى الأخطار المتزايدة والفرص الجديدة الكبيرة المتاحة أمام الدول على هذا الصعيد. وقد أسهمت في هذه المعرفة عناصر لا علاقة لها بالمؤسسات الأمنية مثل:

أ- ارتكاب جرائم بواسطة التحكم الآلي، الأمر الذي يخلق أسبابا ملحة لحماية منظومات المعلومات حتى قبل فحص ضرورات الدفاع المطلوبة في مواجهة الدولة المعادية. ومن أكثر الأعمال شيوعا في هذه المجال: سرقة الأموال، الاحتيال، غسيل الأموال، سرقة الأسرار التجارية، الابتزازات، تشويش وتدمير المعطيات في منظومات المعلومات. وبمقدور التحكم الآلي في جميع هذه الحالات مساعدة المجرمين. ويبدو أن الولايات المتحدة تعتبر جرائم حرب التحكم الآلي بمثابة إحدى الأخطار على الأمن القومي، نظرا لأن هذه الجرائم تهدد النشاطات التجارية والاجتماعية المتزايدة في مجال التحكم الآلي، وتلحق بها أضرارا جسيمة، مما يجعل من

الصعب على الكثير من الشركات مواجهتها. وهناك تقديرات تشير إلى أن أضرار جرائم التحكم الآلي في العالم تزيد عن جرائم تجارة المخدرات. ومن الجدير بالذكر أن إحباط الاعتداءات عبر التحكم الآلي تشغل الكثير من الجهات الاستخبارية مثل المباحث الفدرالية الأميركية.

ب- أعطال في مجال التحكم الآلي: تجسد هذه الأعطال احتمالات وقوع أضرار الاعتداءات في مجال التحكم الآلي. فعلى سبيل المثال في السادس من أيار 2010 نفذ صندوق ائتمان يستخدم رموزا تجارية محوسبة أمر بيع واحد لعقود مستقبلية بقيمة 4.1 مليار دولار، وقد تسبب هذا الأمر في سلسلة من الأحداث التي أفضت إلى إحداث انهيار حاد في سوق الأسهم في الولايات المتحدة – حيث انخفض مؤشر" داو جونز" في غضون دقائق بنسبة 9%. ولا شك أن مثل هذه الحادثة تشير إلى مدى حساسية أسواق المال للنشاطات القائمة على برامج الحاسوب.

وهناك أيضا الأعطال الناجمة عن تعطيل أنظمة الاتصال والحوسبة وهي حالات ليست نادرة، الأمر الذي يجسد مدى الاعتماد المتزايد من قبل السوق والجماهير على مجال التحكم الآلي. ففي إسرائيل على سبيل المثال لا زلنا نتذكر العطل في برنامج الحاسوب في بنك العمال خلال شهر كانون الأول 2010 والذي تسبب في انهيار الاتصالات في جميع أنحاء إسرائيل.

ج- حوار جماهيري وإعلامي واسع: مقالات في وسائل الإعلام، اجتماعات أكاديمية ومقالات مهنية في هذا المجال. إن الحوار يؤكد على الاعتماد الكبير للجماهير في مجال التحكم الآلي في جميع مناحي الحياة ومن ثم الأضرار الجسيمة التي تلحق بها جراء إيقاع أضرار به.

د- حضارة: أفلام، ألعاب حاسوب وكتب مستقبلية والتي تجسد مقدرة هذا المجال في مجال الحرب. وإزاء التقدم التكنولوجي السريع، فإن قسما من الأفلام التي تطرح تبدو في الآونة الحالية قابلة للتنفيذ على أرض الواقع.

استخدام أسلحة التحكم الآلي – عناصر كابحة:

إن السؤال الذي يطرح نفسه إزاء قوة التهديد الكامنة في حرب التحكم الآلي هو: كيف يمكن أن نفسر قلة الاعتداءات التي قامت بها الدول حتى الآن؟ يمكننا القول بادئ بدء أن المقدرة الكافية للحصول على نتائج كبيرة ليست متاحة لجميع الدول، ولا شك أن هذه المقدرة شرطا أساسيا ضروريا، بيد أنه ليس كافيا من أجل اتخاذ قرار الشروع بالعمل. أما بالنسبة للدول التي تمتلك المقدرة، فيبدو أن شن هجوم تحكم آلي يرتبط بمشاكل لا يستهان بها: فهناك ضبابية حول النتائج التي يمكن أن تسفر عن هذا الهجوم، كما أن هناك أيضا أخطارا لا يستهان بها. كما أن استخدام هذا النوع من الحرب يتطلب توفر مبررات وشروط سياسية.

أما بالنسبة للضبابية حول النتائج والإنجازات لمثل هذا الهجوم، فتجدر الإشارة إلى الأسباب التالية:

أ- ليس من الواضح مدى تأثير هجوم التحكم الآلي بسبب قلة المعلومات والخبرة الناجمين عن التاريخ القصير لهذا النوع من الحرب. ومن الممكن أن يكون هناك تأثير محدود لعمليات معينة، في حين أن من المحتمل أن يكون تأثير عمليات أخرى كبيرا جدا مثل إيقاع أضرار غير مرغوب فيها في مؤسسات وأجهزة مدنية. ولقد قال مايكل هايدن – رئيس وكالة ناسا ووكالة المخابرات الأميركية السابق- على هذا الصعيد: "هناك مشكلة في توقع نتائج هجوم التحكم الآلي، إن هذا التوقع أصعب بكثير من توقع نتائج حرب عادية. فلست تستطيع فعل أي شيء في هذا المجال دون أن تحدث ردود فعل في العالم.

ب- من الصعب ترجمة حرب تحكم آلي إلى إنجاز سياسي، في مثل هذه الحرب لا وجود لعمليات الاحتلال لأراض أو أهداف لاستخدامها قاعدة للمفاوضات السياسية في نهاية الحرب على غرار ما هو جار في الحروب البرية.

ج- من الصعب ضمان تواصل الهجوم في مجال التحكم الآلي، ففي حالات كثيرة بمقدور الخصم سد الثغرة وترميم أجهزته بسرعة عالية نسبيا وترميم أضرار الهجوم. وبناء على ذلك من الصعب خلق حالة تتراكم فيها الأضرار مما يفضي إلى خلق ضغوط سياسية، على غرار ما يحدث على سبيل المثال في سلسلة الهجمات

الجوية الإستراتيجية. ويعتقد بعض الخبراء أن هذا الجانب يشكل نقصا كبيرا في مدى تأثير هجمات التحكم الآلي، ويعتقدون أن التوقعات الخاصة به مبالغ فيها. كما أن هناك أخطارا يتعرض لها المهاجم، ولا شك أن هذه الأخطار تعتبر بمثابة عوامل كابحة مثل:

1- خطر الرد على الاعتداء: يمكن للاعتداءات عبر التحكم الآلي أن تعرض دولا لردة فعل مضادة من الدولة المعتدى عليها، ومن الجائز أن يأتي الرد خارج مجال التحكم الآلي. وقد أشار وزير الدفاع الأمريكي لين إلى ذلك في شباط 2011 حينما قال: " لقد طورت بعض الدول مقدرة على اختراق شبكات الحاسوب من أجل جمع المعلومات وليس من أجل إلحاق الدمار والخراب. لقد حاول أكثر من مائة جهاز استخباري التسلل واختراق وكالة المخابرات الأميركية، وكانت جميع تلك المحاولات ترمي للتجسس، هذا رغم أننا لا نستطيع استبعاد أن تكون بعض هذه الدول قد قامت بعملية الاختراق من أجل إلحاق الأذى خصوصا لأنها لا تستطيع شن حرب تقليدية عليها نظرا لمقدرة الردع للجيش الأميركي الأمر الذي يجعل قيام أية دولة بمحاولة اختراق لأجهزة أميركية حساسة يعتبر بمثابة خطر شديد عليها. ورغم أن الدول هي اللاعب الأساسي الذي يملك المقدرة الكافية للتسبب بأضرار عبر شن اعتداءات تحكم آلي، إلا أن من المنطق القول: إنها أقل الجهات التي يمكنها أن تبادر إلى شن اعتداءات قاتلة في الظروف العادية، وذلك على عكس المنظمات الإرهابية. ورغم ذلك على الولايات المتحدة أن تتخذ الاستعدادات اللازمة لمواجهة احتمال أن تصبح حرب التحكم الآلي جزءا من كل حرب تقليدية في المستقبل، مما يتطلب منها أن تمتلك مقدرة تمكنها من حماية نفسها من الدول الأكثر تقدما.

ويبدو أن كفاءة الردع التي يعزيها لين للولايات المتحدة هي مقدرة خاصة نظرا لكونها الوحيدة التي تمتلك المقدرة على الرد بقوة في جميع أنحاء العالم، أي أن البعد الذي يسمح لأية دولة بشن هجوم عبر التحكم الآلي ليس كافيا من أجل الدفاع عنها من الهجمات المضادة التي قد تشنها الولايات المتحدة بصورة تقليدية، وهو الأمر غير المتاح لباقي الدول.

2- "بيت الزجاج": تصبح الأخطار على الدولة المهاجمة أكبر كلما اعتمدت أكثر على مجال التحكم الآلي في استخداماتها، وكلما كان جهازها الدفاعي أضعف. إن الدول الرائدة في مجال شن هجمات التحكم الآلي ترتبط ارتباطا وثيقا بمجال التحكم الآلي وتعتقد أن مقدرتها على الحماية ليست كافية، الأمر الذي يجعلهن مكشوفات أمام الأخطار. وبناء عليه فإن الحماية في مجال التحكم الآلي يمكنها أن تكون أحد الشروط الحيوية للهجوم، كما يجب أن تكون من مصلحتها وقف سباق تسلح التحكم الآلي. بيد أن عدم الثقة بين الدول المختلفة والحوافز التي تتوفر لبعضها لتطوير مقدرة هجومية عبر التحكم الآلي يمكنها أن تتغلب على المصالح وتقود الدولة إلى تعزيز سباق التسلح.

3- أخطار ناجمة عن طرف ثالث – على سبيل المثال دولة حيادية، شركة اتصالات دولية- إن استخدام البنية التحتية لطرف ثالث لشن هجوم قد يعتبر بمثابة مساس بمصالحه. كما أن هناك خطرا آخر يتمثل بالمساس بممتلكات طرف ثالث جراء الاختراقات. وفي الحالات الصعبة قد يؤدي ذلك إلى قيام الطرف الثالث أو المجتمع الدولي بالرد على الاعتداء.

4- أخطار ناجمة عن التحالفات التي يبرمها الخصوم. فعلى سبيل المثال، فإن الضربة التي وجهتها روسيا لأستونيا عام 2007 أثارت لدى حلف الناتو أفكارا جديدة حول ضرورة الدفاع عن أعضائه، وهكذا أدى هجوم غير هام من قبل روسيا إلى ولادة تحالف تحكم آلي ضدها.

5- أخطار في مواجهة المجتمع الدولي. لا يوجد حتى الآن ترتيب فيما يتعلق بالعمليات في مجال التحكم الآلي، ورغم ذلك من الجائز أن تقع هجمات تفضي إلى المساس بحياة بني البشر أو إيقاع أضرار في عمل الدولة بصورة يمكن تفسيرها على أنها خطوة تستدعي شن حرب بناء على القانون الدولي. إن الضبابية القائمة حاليا يمكنها أن تعمل باتجاهين: الأول: اعتبار الوضع الحالي بمثابة فرصة سانحة للعمل في مجال التحكم الآلي والتي يمكنها أن تزول حال تسوية العمل فيها على الصعيد الدولي، والثاني: قد يعمل آخرون على زيادة المساحات الأمنية من أجل الحيلولة دون تعرضهم لردود غير متوقعة من خصوم ومن المجتمع الدولي.

ومن الجدير بالذكر أن المهاجم يواجه مشكلتين أخريين على النحو التالي:

أ- الكشف عن الإمكانيات: شن الهجوم عبر التحكم الآلي يمكنه أن يكشف إمكانيات حساسة أمام جميع الخصوم – وليس فقط أمام الجهة التي جرت مهاجمتها- مما سيمكنهم من حماية أنفسهم مسبقا من تلك الإمكانيات أو استخدامها من أجل شن هجمات من قبلهم. لذا يمكن القول: إن العديد من أسلحة التحكم الآلي تستخدم لمرة واحدة فقط ، أي أنه وحال انكشافها يصبح من الصعب الاعتماد عليها لشن هجمات أخرى.

ب- تضارب المصالح في مجال جمع المعلومات عبر التحكم الآلي. من المحتمل أن تأتي الاعتداءات التي تشنها أجهزة المخابرات عبر التحكم الآلي على حساب عمليات جمع المعلومات، سواء كان ذلك على صعيد تخصيص الموارد أو كان بالنسبة للتناقض القائم بين جمع المعلومات ومهاجمة الأهداف التي تعتبر أصلا مصدرا للمعلومات. وفي الوقت الذي يخفي الاعتداء عبر التحكم الآلي الكثير من المخاطر – مثلما نوهنا آنفا- فإن تطور أساليب جمع المعلومات عبر التحكم الآلي لا يخلق أية مشكلة أبدا لدى الطرف القائم بعملية الجمع. فأساليب جمع المعلومات لا تكتشف، ولا تعمل على تغيير أنظمة الخصم، ولا تثير أية ردود فعل صعبة ضده حتى لو تم اكتشافها.

إرهاب عبر التحكم الآلي:

إرهاب التحكم الآلي هو عملية إرهابية تجري عبر التحكم الآلي أو بواسطته. هناك اتفاق في وجهات النظر بين الخبراء بأن مجال التحكم الآلي يمكنه أن يكون شديد الجاذبية للعمليات الإرهابية، فعلى سبيل المثال قد تقوم جهات إرهابية بتفجير منشأة حيوية مثل مصافي النفط عبر توجيه الضربات لمراكز التحكم والرقابة. هذا وتقوم المنظمات الإرهابية – كالقاعدة- باستخدام مجال التحكم الآلي كوسيلة من وسائل الاتصال الداخلية وللدعاية لكنها لا تستخدمها لشن هجمات.

وفي تعقيبه على هذا الجانب قال نائب وزير الدفاع الأمريكي لين في شباط 2011: إن أكثر ما يقلق الولايات المتحدة هو تمكن المنظمات الإرهابية من الوصول إلى مرحلة تستطيع فيها تشويش وتدمير مجالات

التحكم الآلي الموجودة حاليا تحت رعاية الدول. لقد هددت القاعدة بالقيام بهجمات تحكم آلي بيد أنها لم تفعل ذلك حتى الآن. وأكد على النقاط التالية: من المحتمل أن تطور المنظمات الإرهابية وسائل اعتداءات عبر التحكم الآلي أو أن تشتريها من السوق السوداء. ومن المحتمل أن يتمكن عدد من القراصنة المؤهلين من إلحاق أضرار جسيمة، وفي جميع الحالات سيكون من الصعب اكتشاف المجموعات الإرهابية العاملة في هذا المجال.

ترى ما الذي يمنع المنظمات الإرهابية من تنفيذ عمليات إرهابية بواسطة مجال التحكم الآلي؟ نورد فيما يلي بعض هذه الأسباب:

أ- عدم نضوج المقدرة على القيام بعمليات تسمح بإلحاق أضرار جسيمة.

ب- تفضل المنظمات الإرهابية في الآونة الحالية القيام بعمليات دموية ينفذها الانتحاريون، وتعتبر أن جدوى هذه العمليات أكبر بكثير من العمليات الخفية التي تجري عبر التحكم الآلي .

ج- تضارب المصالح: لا توجد مصلحة للمنظمات الإرهابية في تغيير قواعد اللعب في مجال التحكم الآلي إزاء الاستخدام الواسع له لإدارة المنظمات والاتصال بين الأعضاء، والتوجه إلى جماعات جماهيرية معينة، وتبادل المعلومات.

د- الجدوى: حقا إن تكلفة تطوير أسلحة تحكم آلي نوعية أرخص من تشكيل جيوش تقليدية، بيد أنها أغلى بنسبة كبيرة جدا مقارنة بالقيام بعملية تخريبية.

ويبدو أن السبب الأول المتمثل بعدم نضوج المقدرة على القيام بعمليات تلحق أضرارا جسيمة هي العامل الرئيسي من بين كل تلك العوامل.

ميثاق دولي لتسوية العمليات في مجال التحكم الآلي:

أدت الحاجة إلى ضرورة ترتيب النشاطات والعمليات المسموحة في مجال التحكم الآلي وحماية البنى العالمية إلى بذل جهود عالمية واسعة من أجل بلورة ميثاق دولي، بيد أنه ليس من المعروف متى سيتم توقيعه وإلى أي حد سيكون مجديا. ويقوم بتركيز الجهود الرامية لدفع هذا الميثاق إلى الأمام منظمة الاتصالات التابعة للأمم

المتحدة ITU . وقد دعا رئيس هذه المنظمة في شباط 2010 للتسريع في إقرار الميثاق قبل أن يحدث تدهور وتصل الأمور إلى حد نشوب حرب تحكم آلي.

وتفيد صحيفة واشنطن بوست أنه تم بلورة اتفاقية في منتصف تموز 2010 بشأن العمل على تقليص تهديدات الاعتداء على شبكات الحواسيب. ولا زالت الاتفاقية في طور الاقتراح وقد وقع عليها ممثلون من خمس عشرة دولة ومن ضمنهم الولايات المتحدة والصين وروسيا. ومن بين الخطوات المقترحة: أن تقوم الأمم المتحدة ببلورة قواعد مسلكية مقبولة في مجال التحكم الآلي، وأن تجري عمليات تبادل معلومات بين الدول حول الخطوات التشريعية والإستراتيجية الخاصة بأمن مجال التحكم الآلي، وتعزيز مقدرة الدول الأقل تطورا لتمكينها من الدفاع عن منظومات الحاسوب التي تملكها.

وأضافت واشنطن بوست: أن هذه المجموعة فشلت عام 2005 في التوصل إلى تفاهم مشترك، لكن هذه المرة نجحت - عبر استخدام صيغ قصيرة تحمل مبادئ متفق عليها- في الوصول إلى صيغة متفق عليها.ويقول موظف في الإدارة الأميركية:إن الاتفاقية تعكس تقدما فيما يتعلق بفهم الأطراف لضرورة قيام المجتمع الدولي بمواجهة الأخطار.

وإزاء الخلافات القائمة بين الدول العظمى بشأن محتوى الميثاق وأساليب فرضها بات من الصعب إحراز تقدم حقيقي باتجاه صياغة ميثاق دولي مفصل وفعال. ويمكننا أن نطلع على الخلافات في وجهات النظر من المواقف التي طرحتها الأطراف في السابق، فعلى سبيل المثال وصف موظف أميركي الخلافات بين الولايات المتحدة وروسيا على النحو التالي:"الروس يريدون الحد من الاعتداءات في حين أننا نريد إدانة من يهاجموننا كل يوم". وأوضح في مكان آخر أن روسيا تريد ميثاقا دوليا من أجل منع "سباق التسلح القادم" وتسعى لفرض قيد ورقابة على مجال التحكم الآلي الهجومي على غرار مجال الأسلحة غير التقليدية، أما الولايات المتحدة فلا تؤيد إقامة مؤسسة دولية مستقلة لوضع قيود على حرب التحكم الآلي وتقول: إن أفضل الطرق هي التعاون الفعال وفرض القانون الدولي. ويرى الأميركيون أن هناك صعوبة كبيرة في فرض الميثاق نظرا لأن من المستحيل في مجال

التحكم الآلي التمييز بين العناصر المهاجمة تحت رعاية حكومية وبين النشاطات التي قد يقـوم بهـا أشـخاص. ويبـدو أنهم يخشون من وتيرة تحد مـن مقـدرة الولايـات المتحـدة المتفوقـة في هـذا المجـال وفي نفـس الوقـت لا تحـد مـن النشاطات المعادية لها.

توازن بين العناصر المسرعة والعناصر الكابحة:

يعتبر مجال التحكم الآلي بمثابة ميـدان معـارك جـذاب في أيامنـا هـذه إزاء برمجتـه الخاصـة واتكـال دول وجيوش عليه في أداء وظائفها. ويعزي البعض التاريخ الشحيح للدول المختلفة في مجال شـن الهجـمات عـبر الـتحكم الآلي بوجود كوابح جعلت من الصعب اتخاذ قرار استغلال المجال مـن أجـل شـن الهجـمات إضـافة إلى انعـدام تـوفر الاستعدادات اللازمة لشن مثل هذه الحرب. إن الاستعداد لخوض مثل هذه الحرب يتطلب مقـدرة دفاعيـة ومقـدرة هجومية عالية. كما أن هناك حاجة إلى مؤسسات أمنية ملائمة مهمتها تطوير القدرة على العمل في هذا المجال.

وتسعى الدول في الآونة الأخيرة لتسريع اسـتعداداتها التنظيميـة وتقـيم مؤسسـات أمنيـة للعمـل في هـذا المجال. ولا شك أن هذا السعي يمكنه أن يشير إلى أنها تفترض أن إزالة العوائـق والكـوابح أمـام هجـوم الـتحكم الآلي المدمر ما هو سوى مسألة وقت، وأنها لا تستطيع المخـاطرة بعـدم الاسـتعداد لخـوض هـذه الحـرب في هـذا الميـدان الجديد. إن عملية بناء القوة بحد ذاتها يمكنها أن تسرع تطوير المجال كساحة حرب عسكرية.

وهناك طريقة أخرى للوقوف على مغـزى إقامـة مؤسسـات أمنيـة للـتحكم الآلي وذلـك عـبر المقارنـة بـين تطور المجال في العالم وبين تطـور المجـال الجـوي بوصـفهما مجـالي حـرب عسـكرية. ونـورد فـيما يـلي بعـض الملامـح الأساسية لتطور المجال الجوي منذ ظهور الطـائرات. في عـام 1908 وبعـد خمـس سـنوات مـن أول تحليـق للأخـوين رايــت وقعــا عــلى اتفاقيــة لإنتــاج طــائرات لجــيش الولايــات المتحــدة. وفي الحــرب العالميــة الأولى 1914-1918 ظهرت فوق رؤوس قوات المشاة طائرات جديدة. وفي عام 1917 وإثـر دخـول الولايـات المتحـدة للحـرب أنشـأ فيهـا سـلاح "الخدمـة الجويـة" العسـكرية، والتـي وفـرت الـدفاع والإسـناد للقـوات البريـة وحظيـت بنجـاح في المعـارك

الجوية. وفي نيسان 1918 أنشئ سلاح الجو الملكي البريطاني. وفي الحرب العالمية الثانية 1939-1945 لعبت القوات الجوية البريطانية دورا مركزيا في الدفاع عن بريطانيا وحاربت سلاح الجو الألماني من أجل حيازة التفوق الجوي في سماء بريطانيا، واستخدم كذراع طويلة لشن الهجمات الإستراتيجية في عمق ألمانيا بالتعاون مع قوات الحلفاء.

لقد حظي المجال الجوي بأهمية إستراتيجية خلال النصف الثاني من القرن العشرين إزاء اعتباره مجالا للعمل العسكري من نوع جديد والذي يتيح الفرصة للوصول إلى نقاط ضعف العدو بسرعة ودون الاضطرار لمواجهة القوات البرية المعادية.

لقد قامت عملية تطور المجال الجوي كمجال إستراتيجي على ثلاثة عوامل: التطور التكنولوجي واستغلاله للاحتياجات العسكرية، التحديات القومية الأمنية وإقامة المؤسسات الأمنية التي عملت في مجال التجسيد الفعلي للتكنولوجيا وتجيير كل ذلك لصالح الاحتياجات الإستراتيجية باستخدام الموارد القومية.

وإذا قارنا كل ذلك مع مجال التحكم الآلي على صعيد إقامة المؤسسات في هذا المجال سنجد أن مجال التحكم الآلي لا زال يعيش مرحلة الحرب العالمية الأولى التي عاشها المجال الجوي. إن إقامة مؤسسات أمنية في مجال التحكم الآلي يمكنها أن تحدث ثورة مشابهة على صعيد التفكير والفعل العسكري. وهناك احتمال في هذا المجال لتطور أسرع من التطور الذي شهدناه في المجال الجوي، بيد أن تطبيقه رهن بالحوافز السياسية التي تتأثر بالأحداث الأمنية .

ويبدو أن الدول ستسعى في المستقبل القريب لإحراز التفوق في مجال التحكم الآلي وإقامة أذرع له تعمل خارج هذا المجال من أجل تجسيد أهداف قومية بصورة مستقلة أو بالدمج مع القوات الأخرى على غرار ما حدث مع سلاح الجو.

الفصل الثالث

نظرة عبر الأفق لمدى استعدادات

الدول لمواجهة حرب التحكم الآلي

- - اوباما: "إن البنية الرقمية التي بتنا أسرى لها يوميا هي ذخر قومي إستراتيجي، لـذا يجب أن نضع قضية حمايتها على رأس جدول أعمالنا القومي"

- وثيقة أمريكية: "إن مقدرة الولايات المتحدة في مجال الفضاء والـتحكم الآلي – التـي تسهل حياتنا وتمكننا من القيام بعمليات عسكرية- معرضة للتشويش والاعتداءات".

- الوثيقة تصف عملية حماية مجال التحكم الآلي بوصفه تحديا إستراتيجيا صعبا وغـير طبيعي ويتطلب تعاونا بين السلطة المركزية والمحلية، والقطاع الخاص ومواطني الدولة.

- تـرى الصـين في التكنولوجيـا الرقميـة فرصـة سـانحة لتحسـين مقـدرتها الاسـتراتيجية والاقتصادية والعسكرية ومكانتها بوصفها دولة عظمى يبلغ تعداد سكانها 1.35 مليار نسمة.

يتطرق هذا الفصل إلى الاستعدادات التي تتخذها الدول في مجال التحكم الآلي بما فيها وصف إستراتيجية عملها والمؤسسات الجديدة التي أنشأتها من أجل مواجهة التحديات. وسنطرح بادئ بدء الاستعدادات الأميركية مع التأكيد على الإستراتيجية الجديدة لوزارة الدفاع الأميركية، ثم سنطرح الاستعدادات الفرنسية والبريطانية والألمانية لحماية مجال التحكم الآلي، مع إبراز استعدادات المجال المدني على المستوى القومي، ثم سنتطرق إلى الإستراتيجية الهجومية للصين.

الولايات المتحدة:

تهديدات مجال التحكم الآلي على الولايات المتحدة

تزايد إدراك الولايات المتحدة خلال العقد الماضي للتهديدات الناجمة عن مجال التحكم الآلي من قبل دول ومنظمات إرهابية، ومجرمين آخرين. وقد أدى هذا الإدراك لدفع الأميركيين لبلورة إستراتيجية عمل. وقد كتب الرئيس جورج بوش في مستهل وثيقة "الإستراتيجية القومية لحماية مجال التحكم الآلي" في شباط 2003: "لقد تغيرت أساليب عقد الصفقات والعمليات الحكومية وطرق إدارة الأمن القومي. لقد باتت هذه الأعمال رهنا في عصرنا الحالي بنبى تكنولوجيا المعلومات المسماة مجال التحكم الآلي". إن هذه الوثيقة التي أعدها البيت الأبيض تشير إلى الارتفاع الدرامي في تهديدات مجال التحكم الآلي وتشير إلى اتجاهات عمل لمواجهة هذه التهديدات. ومنذ ذلك الحين تزايدت التهديدات في هذا المجال على الولايات المتحدة.

لقد وصف الرئيس الأميركي باراك أوباما تهديد مجال التحكم الآلي بأنه أحد أخطر التهديدات على الأمن القومي الأميركي وعلى الاقتصاد الأميركي. وقال: "إن البنية الرقمية التي بتنا أسرى لها يوميا هي ذخر قومي إستراتيجي، لذا يجب أن نضع قضية حمايتها على رأس جدول أعمالنا القومي". وأكد أن الولايات المتحدة تعتمد على مجال التحكم الآلي بدءا من الجيش وحتى شبكة الكهرباء، وأعرب عن قلقه من احتمال شن هجوم على الولايات المتحدة في هذا المجال،وقال: "إن ازدهار أميركا الاقتصادي في القرن الحادي والعشرين رهن بحماية مجال التحكم الآلي".

أبرزت وثيقة "إستراتيجية الأمن القومي" للبيت الأبيض في شهر أيار 2010 تهديد التحكم الآلي على الولايات المتحدة وجاء فيها: "إن مقدرة الولايات المتحدة في مجال الفضاء والتحكم الآلي - التي تسهل حياتنا وتمكننا من القيام بعمليات عسكرية- معرضة للتشويش والاعتداءات". وسنشير في إطار تقييمنا نموذجا لمدى الاعتماد العسكري الإستراتيجي على مجال التحكم الآلي إلى شبكة Global information Grid-GIG والتي تضم كما متنوعا وهائلا من وسائل الاتصالات بما فيها أقمار صناعية ذات انتشار عالمي. والشبكة تمكن الولايات المتحدة من نقل معلومات بين نقاط مختلفة على الأرض بسرعة وأمان ودقة، مما يمكنها من نقل الأوامر لقواتها، لتوجيه قنابل ذكية إلى أهدافها باستخدام أجهزة جي.بي.إس، والسيطرة على الطائرات دون طيار من أقصى العالم وغيره. وإذا أصيبت هذه الشبكة بأضرار، فسوف تفقد الولايات المتحدة هيمنتها في ميادين القتال العالمية.

أشار نائب وزير الدفاع لين خلال شهر شباط 2010 إلى ثلاثة تهديدات أساسية في مجال التحكم الآلي: التجسس، تشويش - كالهجوم الذي يحجب الخدمة- والهجمات التي ترمي إلى زرع الدمار. وهو يعتقد أن التهديد الأخير هو أخطرها وأن هذا التهديد بدأ يشق طريقه في الآونة الحالية، حيث باتت الوسائل متوفرة، وكذلك النوايا لاستخدامها. ويمكننا أن نتخيل هجوما على الشبكات العسكرية والبنى التحتية الحساسة مثل شبكة المواصلات، وقطاع الطاقة، مما سيلحق أضرارا اقتصادية جسيمة،ودماراً مادياً بل وفقدان حياة الأشخاص. إن الانتقال البادي في مجال التحكم الآلي من التشويش إلى الدمار يعكس ارتفاعا في سلم تصعيد التهديدات، أي أنه كلما تطورت التهديدات كلما أصبحت وسائل تنفيذها أكثر.

وأضاف: "نحن نعيش لحظة إعداد على صعيد تهديدات التحكم الآلي، حيث يجري تطوير المزيد من وسائل الدمار، بيد أن هذه الوسائل لم تصل بعد إلى مرحلة التنفيذ الفعلي، كما أن اللاعبين الأشرار لم يضعوا أيديهم بعد على تلك الوسائل ذات المقدرة الهائلة على الدمار. بيد أن هذا الوضع لن يظل علي ما هو عليه إلى الأبد. فالمنظمات الإرهابية والدول المعادية ستتمكن من الحصول على مثل هذه الوسائل. لذا فإن من واجبنا أن

نصنع مقدرة دفاعية قبل حدوث ذلك. لا يزال أمامنا بعض الوقت الذي لا ندري ما مدى هامشه بعد من أجل تعزيز شبكاتنا ضد التهديدات الخطرة.".

ويقول لين: يمكننا القول على الصعيد النظري أن الهجمات المدمرة عبر التحكم الآلي لن تنفذ أبدا، بيد أن التاريخ يعلمنا أن الوسائل التي تم استخدامها للحرب ولم تستخدم هي وسائل قليلة جدا، وبناء عليه يتوجب على الولايات المتحدة أن تكون على أهبة الاستعداد للدفاع عن نفسها ضد جميع وسائل حرب التحكم الآلي المحتملة.

المؤسسات التي أنشأتها الولايات المتحدة من أجل حماية مجال التحكم الآلي:

يشرف البيت الأبيض على الرؤيا الشمولية والإستراتيجية الأميركية للدفاع في مجال التحكم الآلي. وإلى جانب الرئيس الأميركي أوباما يشرف على هذا المجال هوارد شميدت منسق عمليات الأمن في مجال التحكم الآلي والمساعد الخاص للرئيس. لقد تم تعيين شميدت في كانون الأول 2009، وهو مسؤول أيضا عن تنسيق وتركيز سياسة الإدارة الأميركية وعلى المساعدات المقدمة للرئيس في إدارة الأزمات في حماية مجال التحكم الآلي.

ويلعب مكتب أمن الوطن دورا مركزيا في تجسيد إستراتيجية أمن مجال التحكم الآلي. وشعبة حماية التحكم الآلي هي الجهة المسؤولة في المكتب عن هذه القضية. وترى هذه الشعبة أن هدفها يتمثل في "العمل بالتعاون مع جهات في القطاع العام والخاص ومع جهات في العالم من أجل حماية مجال التحكم الآلي والتجهيزات الأميركية المتعلقة به. ويتمحور عملها حول حماية الشبكات الفدرالية وحماية البنى الحيوية. وتشرف الشعبة على تجسيد خطة للرد الدفاعي على أي هجوم. والخطة تضم القضايا الإدارية والإجراءات والبروتوكولات التي يجب انتهاجها في مواجهة الأحداث غير العادية التي يتم اكتشافه في مجال التحكم الآلي. كما أنها مسؤولة عن برنامج إدارة الأخطار **Cyber-Risk Management Programs** والتي تقوم بوضع خارطة للأخطار والعمل على تقليصها مع دراسة مدى جدواها. كما تقوم الشعب بالتنسيق بين

السلطات الرسمية ومشاركة المعلومات بين الجهات المختلفة – بما فيها القطاع الخاص، في مجال التحذير من عمليات معادية في مجال التحكم الآلي. كما أن هناك تعاونا وطيدا بينها وبين قيادة التحكم الآلي في وزارة الدفاع.

وتعتبر وزارة الدفاع مسؤولة عن دفاع وهجوم التحكم الآلي في المجال العسكري وعلى المساعدات للجهات المدنية. ولهذا الغرض أنشئت في أيار 2010 قيادة التحكم الآلي بوصفها جزءا من القيادة الإستراتيجية في وزارة الدفاع. وقد أفاد قائد القيادة الجنرال ألكسندر في شهادته أمام الكونجرس: أن قيادته مسؤولة عن تنفيذ مهام التحكم الآلي الملقاة على عاتقها من أجل ضمان حرية العمل في مجال التحكم الآلي وتقليص الأخطار التي يتعرض لها الأمن القومي. ومن ضمن مهام هذه القيادة ما يلي:

أ- قيادة العمليات الدفاعية عن الشبكات العسكرية ووزارة الدفاع.

ب- خلق سلسلة قيادة واضحة لاتخاذ القرارات في مجال حرب التحكم الآلي. وسلسلة تفعيل قيادة التحكم الآلي هي: الرئيس الأميركي، ووزير الدفاع، ورئيس القيادة الإستراتيجية، ورئيس قيادة التحكم الآلي.

ج- خلق تعاون مع جهات خارج الجيش ووزارة الدفاع – الوزارات الحكومية الأخرى، والقطاعات الخاصة- وخارج الولايات المتحدة فيما يتعلق بحرب التحكم الآلي.

د- على الصعيد التنفيذي: تأطير مهام التحكم الآلي والتأثيرات الأمنية العالمية، وتوجيه العمليات في شبكة المعلومات العالمية، تنفيذ مختلف العمليات في مجال التحكم الآلي.

هـ - خلق معرفة لعمليات التحكم الآلي ضد الولايات المتحدة والتحذير من الأعداء.

و- العمل كممثل للجيش في مجال التحكم الآلي خلال الاتصالات مع الجهات المختلفة ومن ضمنها أجهزة المخابرات الأخرى والشركات الأميركية والأجنبية.

إن جماعة المخابرات الأميركية تعتبر بمثابة عامل هام في جهاز أمن التحكم الآلي. وتشير وثيقة إستراتيجية جماعة المخابرات الأميركية التي أعدت في آب 2009 إلى أن تعزيز مقدرة التحكم الآلي هي إحدى المهام الخمسة الأولى التي تحتل رأس قائمة اهتمامات المخابرات الأميركية. إن مجال التحكم الآلي هو مساحة واسعة لعمل المنظمات الاستخبارية على صعيد جمع المعلومات، والهجوم والمساعدة والدفاع. وتعمل أجهزة الأمن الأميركية – مثل جهاز المباحث الفدرالية- في مجالات أخرى كالمجال الجنائي، ومن ضمنها إحباط عمليات الغش التي تجري في مجال التحكم الآلي. كما ألقي على عاتق هذه المنظمات أيضا مهمة تعزيز استغلال تكنولوجيا المعلومات من أجل تحسين أدائها الداخلي، مثل تحسين تأطير المعلومات والمعرفة، وإدارة المهام التنظيمية للجماعات الأمنية، ومكننة إجراءات الشراء وغيره. ويبدو أن الجهات الاستخبارية والجيش تعزز جهودها لتطوير مقدرة حرب في مجال التحكم الآلي. ومن الجائز أن هذا الاتجاه يتطلب أو سيتطلب تنظيم تقسيم المسؤولية والصلاحيات بينها في مجال حرب التحكم الآلي. ومن الجدير بالذكر أن وكالة الفضاء الأميركية "ناسا" تعتبر بمثابة جزء من جماعة الاستخبارات الأميركية وأيضا جزء من الجيش ووزارة الدفاع الأميركية.

إستراتيجية الولايات المتحدة لضمان أمن مجال التحكم الآلي:

جاء في وثيقة "الإستراتيجية القومية لحماية مجال التحكم الآلي" التي نشرها البيت الأبيض في شباط 2003 أن هدف الإستراتيجية هو: "توفير إطار للدفاع عن البنى الحيوية الاقتصادية والأمنية وأسلوب الحياة الأميركية". وتصف الوثيقة عملية حماية مجال التحكم الآلي بوصفه تحديا إستراتيجيا صعبا وغير طبيعي، ويتطلب تعاونا بين السلطة المركزية والمحلية، والقطاع الخاص ومواطني الدولة. وفي هذا الإطار دعا الرئيس الأميركي آنذاك – جورج بوش- القطاع الخاص للمشاركة مع الحكومة في تجسيد الإستراتيجية نظرا لأن العمل المشترك هو وحده الكفيل بإبقاء مجال التحكم الآلي آمنا ومحميا في المستقبل. وعلى رأس قائمة اهتمامات الإستراتيجية تقف القضايا ذات العلاقة بالأمن القومي والمعرضة لمجال التحكم الآلي، البنى القومية الحيوية،

والقطاعات الضعيفة والمصانع الكبيرة. وقد منحت أولوية أقل لحماية قطاعات الأعمال الصـغيرة والمصـانع الصـغيرة، ومنحت الدرجة الأقل في الحماية لحماية مجال التحكم الآلي العالمي.

لقد وضعت الإستراتيجية المذكورة لاستخدامها كإطـار لـدمج القـوات وتوزيـع المهـام بـين جميـع الجهـات العاملة من أجل أمن مجال التحكم الآلي في الولايات المتحـدة، ومـن ضـمنها: مكتـب منسـق ومسـاعد رئـيس مجـال التحكم الآلي، شعبة أمن التحكم الآلي ووزارة أمن الوطن، قيادة التحكم الآلي في وزارة الدفاع، المخـابرات، جهـات في وزارة العدل وغيرها. كما كلفت الوزارات الحكومية بالتنسيق بين جميع الجهات ذات العلاقة في الدولة لحماية البنى الحيوية في مجال مسؤولياتها، فعلى سبيل المثال تعتبر وزارة المالية مسؤولة عن حماية البنى الحيوية في سـوق المـال. ووزارة الطاقة مسؤولة عن حماية منشآت الطاقة الهامة وغيره.

وبصورة عامة تعتبر أهداف الإستراتيجية سارية المفعول في وقتنا الحاضر أيضا. إن التغيير الـذي طـرأ عـلى هذا المجال يتمثل في القفزة الكبيرة التي حققتها الولايات المتحدة خلال السـنوات القليلـة الماضـية في تنظـيم نفسـها لخوض ومواجهة حرب التحكم الآلي، وخصوصا في أعقاب تجسد قسم من التهديدات. وهناك تغيـير كبـير أيضـا يـبرز على صعيد التعامل الأميركي مع حماية مجال التحكم الآلي خارج حدودها.

لقد دشن البيت الأبيض في أيار 2011 "الإستراتيجية الدولية لمجال التحكم الآلي". ومن الجـدير بالـذكر أن الإستراتيجية التي طرحتها وزيرة الخارجية الأميركية هيلاري كلينتون تكمـل وتحسـن الإسـتراتيجية السـابقة في مجـال التحكم الآلي خارج حدود الولايات المتحدة، وهي تضفي أهمية كبيرة على هذا المجال في سياسـة الخارجيـة، والـدفاع والتجارة الأميركية. وبناء على الإستراتيجية الجديدة فإن على الولايات المتحدة أن تعمل من أجل تحسين وتطوير بنية معلومات عالمية آمنة، وصادقة وحـرة، بصـورة تتـيح تجـارة دوليـة،وتعزيز الأمـن القـومي، وتشـجيع حريـة التعبـير والتحديث، وذلك عبر بناء ثقافة مسلكيات مسؤولة، وتوجيه من قبل الدولة، وخلق شراكة ودعم لسـلطة القـانون في مجال التحكم الآلي.

هذا ويوجد للولايات المتحدة ثلاثة تقديرات بارزة لحماية مجال التحكم الآلي خارج حدودها والتي يجب على إستراتيجيتها أن تدعمها:

أ- تعزيز أمن الولايات المتحدة وحلفائها. إن الولايات المتحدة تدرك أنها لن تتمكن من إحراز الأمن في مجال التحكم الآلي دون تعاون، نظرا لأن الشبكات مربوطة ببعضها البعض، بما فيها الشبكات الأمنية على غرار ما هو حادث بين الدول الأعضاء في حلف الناتو. ولا شك أن هناك العديد من الفرص في هذا الجانب من مجال التحكم الآلي – إمكانية الحصول على تحذيرات مسبقة- بيد أنه يشتمل أيضا على الكثير من الأخطار.

ب- يوجد للولايات المتحدة ولحلفائها مصالح اقتصادية، اجتماعية، سياسية، وأمنية رهن بالشبكات العالمية. فعلى سبيل المثال يمكن عبر انترنت محمى وتعاون تحسين التجارة الأميركية في شتى أنحاء العالم، وحماية الممتلكات الروحية، وتحسين مقدرة الولايات المتحدة على مواجهة الجرائم في مجال التحكم الآلي وبواسطته.

ج- تسعى الولايات المتحدة لإشاعة القيم الأميركية مثل حرية التعبير وحقوق المواطن في مجال التحكم الآلي وبواسطته. وقد قال الرئيس الأميركي في مستهل الوثيقة الإستراتيجية آنفة الذكر أن مجال التحكم الآلي والتكنولوجيا التي يتيحها تسمح للأشخاص من جميع القوميات والأجناس، والتطلعات والأديان للتعاون والازدهار والاتصال أكثر من أي وقت مضى. لقد تم تعيين العديد من الوزارات لتطبيق الإستراتيجية آنفة الذكر: وزارة الخارجية، الدفاع، أمن الوطن، التجارة والعدل. كما تم تعيين كريس منسقا للإستراتيجية.

إن إستراتيجية وزارة الدفاع الأميركية وتطبيقها موجودة في طور الدراسة النهائي، بل وقد تم تطبيق أقسام منها. وهذه الإستراتيجية متميزة وعصرية وتطرح من قبل الأميركيين بصورة مفصلة لا شبيه لها في الدول الأخرى. وتنخرط هذه الإستراتيجية في إستراتيجية البيت الأبيض التي أشرنا إليها آنفا.

أشار نائب وزير الدفاع لين إلى أن هذه الإستراتيجية تقوم على خمسة أسس رئيسة هي:

أ- اعترفت وزارة الدفاع عام 2010 رسميا بمجال التحكم الآلي بوصفه مجال حرب مثل المجال البري، الجوي، البحري والفضائي. وهذا يعني أنه يتوجب على الجيش أن يعمل في هذا المجال الجديد على غرار مجالات الحرب التقليدية الأخرى من أجل الحفاظ على الأمن القومي. وبناء عليه يتوجب على الجيش أن يعد العدة ويتدرب ويجهز أذرعته بالتجهيزات اللازمة من أجل تنفيذ مهامه في مجال التحكم الآلي. ولهذا السبب أنشئت قيادة مجال التحكم الآلي وعمد كل ذراع من أذرعته إلى تشكيل هيئات للعمل في المجال.

ب- شبكات الجيش ووزارة الدفاع مجهزة بمنظومات دفاع فعالة – وذلك لتمييزها عن شبكات الدفاع السلبية العاملة فقط في أعقاب اكتشاف اختراق. وشبكة الدفاع الفعالة تقوم على عمل ديناميكي فيه تعمل بسرعة الشبكة مع استخدام أجهزة تنقية،وبرامج ومعلومات استخبارية لاكتشاف البرامج الشريرة ووقف عملها قبل أن تنجح في إلحاق الأضرار. ونظرا لأن عمليات الاختراق لا تكتشف دائما داخل حدود التحكم الآلي في الدولة، فإن الدفاع الفعال يعمل من أجل اصطياد المخططات الشريرة في المجال.

ويقول نائب وزير الدفاع الأميركي لين: رغم أنه لا يمكننا القول أن هناك شبكة آمنة بنسبة 100% إلا أن شبكة الدفاع الفعالة حسنت الوضع الأمني في شبكات وزارة الدفاع. إن منظومة الدفاع الخاصة بالتحكم الآلي التي تشرف عليها وزارة الدفاع تقوم على ثلاث طبقات دفاعية: الطبقتان الأوليان تقومان على شبكات دفاعية وفرتها شركات تجارية عبر منظومات برامج دفاعية متنوعة – Anti-virus' firewall – أما الطبقة الثالثة فتقوم على مقدرة الجهات الاستخبارية القومية. ومهمة هذه الطبقة توفير الدفاع الفعال، ونقل معلومات حول الهجمات التي ستشن إلى أجهزة الحماية في مجال التحكم الآلي القومي، والتنسيق بين القوى العاملة في المجال القومي وإدارة المعركة من خلال نظرة شمولية.

ج- ضمان حماية بنية التحكم الآلي الحيوية في الدولة التي يعتمد عليها الجيش أيضا عبر التعاون مع القطاع المدني. وقد أكد لين أهمية الدفاع عن بنى التحكم الآلي المدنية والتي دونها لا تستطيع شبكات الكهرباء ووزارات الحكومة العمل. وقال: لهذا السبب فإن مهمة وزارة الأمن الداخلي في مجال التحكم الآلي حاسمة

ويتوجب على وزارة الدفاع أن تساعدها على هذا الصعيد. فعلى سبيل المثال إذا وقعت كارثة طبيعية، مثل الأعاصير، فإن السلطة الفدرالية لمعالجة الكوارث القومية تستخدم قوات الجيش، وبنفس الصورة يجب أن تكون قوات الجيش جاهزة وعلى استعداد للاستجابة لدعوة الزعماء المدنيين من أجل المساعدة في الدفاع عن الشبكات والبنى الحيوية، ودعم نشاطات الجهات الحكومية. وأكد لين أن الموارد ستكون تحت السيطرة المدنية في جميع الحالات التي سيقدم فيها الجيش مساعداته للسلطات المحلية، وسيتم استخدامها وفقا للقوانين المدنية. وبناء على هذا الوضع تم بناء شراكة رسمية في تشرين الأول 2010 بين وزارة الدفاع ووزارة الأمن الداخلي في مجال التحكم الآلي.

وفي إطار التجارب الجارية نقلت تكنولوجيا عسكرية ومن ضمنها في مجال الحماية الفعالة لاستخدامها من قبل وزارة الأمن الداخلي للدفاع عن الشبكات الحكومية، كما تم تأسيس أطر للتخطيط المشترك لتبادل الطاقة البشرية بين الوزارات. ويقول لين: إن هذه المبادرات حسنت إلى حد كبير مقدرة الوزارات الحكومية في مواجهتها لتهديدات التحكم الآلي.

ويتضح من الشهادة التي أدلى بها قائد قيادة التحكم الآلي الجنرال ألكسندر أن صلاحيات وزارة الدفاع تتسع في حالات الطوارئ على حساب وزارة الأمن الداخلي في كل ما يتعلق بالدفاع عن الأمة، الأمر الذي يعني أنها تتسع أيضا في حالة حماية مجال التحكم الآلي المدني. وتقوم الإستراتيجية على فهم أن بنى التحكم الآلي المدنية حيوية لعمل الجيش، وأن من المستحيل حمايتها دون تدخل الجيش.

د- بناء "الحماية الشاملة" والتعاون مع الحلفاء يتيح الفرصة للإشراف بصورة مشتركة على شبكات الحاسوب من الاختراق على غرار منظومات الدفاع الجوية المشتركة التي تتيح الفرصة لتلقي إنذار بشأن الهجمات المحتملة. ومن الجدير بالذكر أن الوثيقة الاستراتيجية للبيت الأبيض التي وضعت في أيار 2011 تتطرق إلى هذه القضية. إن أحد أهداف الاستراتيجية المتعلق بالمجال العسكري هو بناء تحالفات عسكرية لتحسين التحالفات القائمة، بغية مواجهة التهديدات المحتملة في مجال التحكم الآلي. وليس أدل على ذلك من

الجهود التي تبذلها الولايات المتحدة من أجل تشكيل ائتلاف تحكم آلي في حلف الناتو. وقد حظيت هذه الجهود بزخم كبير خلال المؤتمر الذي عقد في إدارة الناتو خلال شهر تشرين الثاني 2010، حيث تم الاتفاق على منح أولوية أعلى لمواجهة تهديدات التحكم الآلي، كما اتخذ قرار بتقديم موعد إقامة مركز ردود التحكم الآلي للناتو NATO Cyber Incident Response Center بثلاث سنوات مقارنة بالتخطيط الأساسي، بحيث يصبح عمليا عام 2012.

هـ- مشاركة القطاع الخاص. وبهذه الطريقة يمكن أن نضمن أن الموارد التكنولوجية والبشرية الأفضل في الدولة ستخصص لمجال حماية مجال التحكم الآلي مثلما تعمل الولايات المتحدة في مجالات أخرى.

لقد اعتمد الجنرال ألكسندر في شهادته أمام الكونجرس في نيسان 2010 على وثيقة "الاستراتيجية العسكرية للعملية في مجال التحكم الآلي" التي وضعت في نهاية 2006، والتي كلفت بتنفيذها حاليا قيادة التحكم الآلي، وقال: إن هدف الاستراتيجية هو نيل التفوق في مجال التحكم الآلي من أجل ضمان حرية العمل الأميركية وحرمان الأعداء من هذه الحرية. ويجب إحراز هذا الهدف عبر توحيد الشبكات، والدفاع، وجمع المعلومات والهجوم في مجال التحكم الآلي. ولا شك أن من الصعب نيل التفوق في البيئة الحالية بيد أنها لا زالت ممكنة.

وأضاف: حقا يجب في المرحلة الأولى تطوير المقدرة الدفاعية، بيد أن تعرض الولايات المتحدة للاعتداءات لا يتناقض وهدفها في حيازة التفوق، بيد أن هذا الأمر يتطلب منها تطوير مقدرة هجومية. ومن بين الأسئلة التي وجهها السناتورات الأمريكيون إلى ألكسندر ورد عليها وراء الأبواب المغلقة: هل سيكون بأيدي قيادة التحكم الآلي وسائل هجومية قوية في مجال التحكم الآلي؟ وهل وجود هذه الوسائل سيشجع آخرين على تطوير وسائل مماثلة؟ وما هو مستوى التأكيد الأمني الذي يجب عليه أن يحدد به هوية المعتدي قبل أن يرد على الهجوم؟

إن التعاون بين القطاعين الأمني والخاص هـو مسـألة مركزيـة في الإسـتراتيجية الجديـدة لـوزارة الـدفاع في مجال التحكم الآلي. ويقول لين: "إن الإستراتجية الشاملة هـي حقـا معلـم طريـق هـام بيـد أن الحكومـة لا تسـتطيع الدفاع عن الدولة وحدها. إن الدفاع في مجال التحكم الآلي ليست مهمة عسكرية مثل الدفاع في الفضاء، حيث تلقـى كامل المسؤولية والتبعة على الجيش. فالقسم الحاسم من البنى القوميـة الحرجـة بمـا فيهـا الإنترنـت موجـود بأيـدي خاصة". وبناء على ذلك فإن حماية الشبكة تتطلب تعاونا بين القطاع العام والقطاع الخاص.

وقد عدد ألكسندر ثلاث مسارات للتعاون بين القطاع العام والخاص والتـي يجـب العمـل عـلى دفعهـا إلى الأمام من أجل تحسين حماية الولايات المتحدة في مجال حرب التحكم الآلي:

-المسار الأول: التعاون في مجال المعلومات. يتمتع مزودو الاتصالات والإنترنت برؤيا ممتازة على صعيد ما يحدث في الشبكات العالمية. وبمقدورهم اكتشاف حركة الهجوم في شبكاتهم، وفي الكثير من الحالات بمقدورهم تزويد زبائنهم بإنذار مبكر، كما أنهم يتمتعون بصورة عامة بمقدرة على تفعيل شبكاتهم بأفضل الطرق الممكنة للرد على أي هجوم. ووزارة الدفاع تعمل باستخدام تكنولوجيا رئيسـة وشركـات أمنيـة مـن القطـاع الخاص،وهنـاك عمليـة تبـادل معلومات لتحسين الأمن والمقدرة في مجال التحكم الآلي. ويقوم مدراء رفيعو المسـتوى مـن الشركـات بـالاجتماع مـع شخصيات رفيعة في وزارة الدفاع، ووزارة الأمن الداخلي ومكتب رئيس الأجهزة الأمنية الأمـيركي. إن الشراكـة الخاصـة والعامة لا تسهم فقط في اكتشاف نقاط الضعف في الشبكة، بل أيضا تشـجع العمـل في القطاعـات الحكومية،وتـدفع بخبراء في الصناعات لمواجهة الأخطار الأمنية قبل وقوع الضرر.

-المسار الثاني: التعاون لدعم وتعزيز هندسة شبكة الإنترنت – البنية، التنظيم، الترتيب الوظيفي، القواعـد العامة، منظومات الدفاع وغيره. وإزاء عدم التوازن بين الدفاع والهجـوم في الشـبكة، وفي سـبيل العمـل عـلى تقلـيص التفوق الذي يتمتع به قراصنة الشبكة، فإن وزارة الدفاع الأميركية تطلب مساعدة القطاعات العلمية لتعزيز هندسة الشبكة بما فيها ترميم منظومات الحمايـة والتحقـق عـلى مسـتوى رفيـع: في المـواد، وأجهـزة التشـغيل وبروتوكـولات الشبكة.

ويقول لين: "يجب على إستراتيجية التشخيص الموثوق في الشبكة" - والتي تعتبر بمثابة مبادرة من البيت الأبيض- أن تضع حجر الأساس لمستقبل أكثر أمنا في الشبكة. حقا أن البنية الرقمية لن تتغير بين عشية وضحاها، بيد أن من الممكن إحداث تغيير هندسي على المدى البعيد يمكننا عبره إصلاح إحدى نقاط الضعف المثيرة للمشاكل في تكنولوجيا اليوم.

ويقول لين: " كي نتمكن من دفع الجهود إلى الأمام، قررت وزارة الدفاع الأميركية إضافة نصف مليار دولار لتمويل أبحاث جديدة بشأن القضايا ذات العلاقة بأمن مجال التحكم الآلي بما فيها تمويل أولي لشركات خاصة تعمل في مجال تطوير تكنولوجيا ذات استخدام مزدوج قادرة على خدمة الاحتياجات الأمنية في مجال التحكم الآلي.

وأضاف: "إن القطاع الحكومي مصاب بالتباطؤ، فعلى سبيل المثال احتاجت وزارة الدفاع الأميركية في أيامنا هذه إلى واحد وثمانين شهرا من أجل استيعاب منظومة حاسوب في حين أن جهاز أيفون طور خلال أربعة وعشرين شهرا فقط. يجب إغلاق الهوة القائمة بين القطاع الحكومي والقطاع الخاص.

كما كشف لين النقاب عن وجود برامج لتبادل المعلومات والطاقة البشرية بين القطاع الحكومي وصناعة تكنولوجيا المعلومات. إن وزارة الدفاع معنية بالحصول من هذه الصناعات على مدراء رفيعي المستوى كي تدخل إليها الإمكانيات والقدرات الموجودة في الصناعة، الحصول على خبراء من الصناعات قادرين على مواجهة التحديات التي تواجه وزارة الدفاع بصورة مباشرة. كما تم الإعلان عن وجود برنامج لاستغلال الخبرة المكتسبة في مجال التحكم الآلي في أوساط الحرس الوطني وجهاز الاحتياط ، فالكثير من الجنود الذين يخدمون في هذه الهيئات يعملون كمدنيين في مجالات المعلومات التكنولوجية في العالم. وكي نتمكن من استغلال خبراتهم بفعالية كبيرة يجب أن ننشئ في هذه الهيئات وحدات هدفها القيام بمهام تحكم آلي.

-المسار الثالث: وهو المسار الذي يتوقع لين أن يتسم بالتعاون بين القطاع الحكومي والخاص، أي توسيع الدفاع الفعال بحيث يصل إلى الشبكات الخاصة المرتبطة ببنى حيوية في الجيش والاقتصاد. إن مقدرة

الولايات المتحدة الاستخبارية جعلت القطاع الحكومي يمتلك قدرا هائلا من المعلومات السرية حول أخطار تحكم آلي معينة. إن التكنولوجيا التي طورتها وزارة الدفاع بناء على احتياجات الشبكات الأمنية – والتي من المفروض أن تواجه هذه الأخطار- يمكنها أن تعزز الفعالية الأمنية في مجال التحكم الآلي بالنسبة للقطاع الخاص على حد كبير جدا.

لقد قامت وزارة الدفاع بتوزيع معلومات غير سرية على شركات أمنية خاصة من الشركات التي تحتوي شبكاتها على معلومات حساسة فيما يتعلق بتهديدات التحكم الآلي عليها. إن السؤال الملح الذي تطرحه الدول على نفسها هو: كيف يمكن أن نشارك بالمعلومات التكنولوجية السرية شركات تدعم الجيش والاقتصاد بغية تحسين أمن التحكم الآلي لديها؟ إن الأمر يتعلق بالمصالح، حيث أن بمقدور الشركات والمصانع التابعة للبنى الحيوية أن تحقق أرباحا كبيرة من الدفاع الفعال الذي ستحصل عليه. ولا شك أن بحوزة وزارة الدفاع التكنولوجيا والمقدرة على تطبيق مثل هذا الدفاع والحماية على الصعيد المدني. إن أحد التحديات الهامة يتمثل في تطوير إطار سياسي وقانوني يسمح بذلك.

لقد أثنى لين على التعاون بين القطاعين العام والخاص ما قبل عام 2000 توطئة لمواجهة فيروس "باج" حيث جرى الحديث آنذاك عن تهديد عالمي على كل ما هو رقمي، لكننا الآن نواجه لاعبين شديدي الخطورة . إن تحسين المسار الثالث – البنى المدنية الحساسة- هو أشد التحديات التي نواجهها.

بدا أن نائب وزير الدفاع يتطرق إلى تدخل وزارته في المجال المدني للتحكم الآلي بحذر كبير، وخصوصا في حديثه عن تدخل الجيش في الدفاع عن البنى المدنية الحساسة – الأساس الثالث أعلاه. وذلك إزاء الخلافات التي نشبت في الماضي بشأن تدخل الجيش في القطاعات المدنية. فعلى سبيل المثال أثارت عملية حساب أخطار التحكم الآلي التي قامت بها وكالة MSA عام 2009 بناء على طلب من حكومة أوباما معارضة في وزارة الأمن الداخلي.

ويقول "رود بكستروم" – الذي استقال من منصبه كمدير عام للمركز القومي لحماية المعلومات: إنه يخشى من أن تؤدي عملية حساب الأخطار آنفة الذكر إلى تمكين NSA من القيام بفحص كل بريد الكتروني أو رسالة ما أو أن تفتش في "google" وراء كل موظف أميركي يقوم بالعمل على الانترنت. من المفروض أن تقوم المخابرات الأميركية بجمع معلومات حول ما يحدث خارج الولايات المتحدة، ولا يجب أن تقوم بالسيطرة على عملية نقل المعلومات داخل الدولة إلى هذا الحد.

وهناك نموذج آخر يمكننا التطرق إليه، ففي أعقاب إعلان وزير الدفاع في حزيران 2009 عن نية تشكيل قيادة التحكم الآلي أطلقت في واشنطن العديد من الانتقادات جراء قيام جهة عسكرية بمعالجة مسائل حماية شبكات الحاسوب المدنية مما سيعرض المعلومات الموجودة فيها للانكشاف أمامه. كما ثارت انتقادات حول إمكانية أن يمنح الجيش أولوية لحماية الشبكات المدنية عن الشبكات العسكرية.

إن المعلومات الخاصة بالإستراتيجية الأميركية تبرز بشكل واضح الطابع الدفاعي للنظرية الأميركية. وهذه النظرية ترمي للحفاظ على الممتلكات الوطنية وعلى مكانة الولايات المتحدة بوصفها دولة عظمى والتي تقوم على التفوق التكنولوجي تجاه الأعداء والخصوم والمنافسين، مثل الصين. ورغم ذلك فإن ميدان حرب التحكم الآلي يشمل عمليات دفاعية وهجومية في نفس الوقت، ويبدو أن الولايات المتحدة تتفوق على أية دولة أخرى في مجال الهجوم والتواجد في المجال.

إن شن الهجوم في مجال التحكم الآلي هو من مهام قيادة هذا المجال والتي لم يتم توضيحها بالتفصيل من قبل الجهات الأمنية الأميركية لأسباب معروفة.

وفي الكلمة التي ألقاها مايكل هيدن خلال مؤتمر الحماية Black hat في تموز 2010 في لاس فيجاس قال: إن قيادة التحكم الآلي عاكفة طيلة الوقت على العمليات الدفاعية، وأن الجيش الأمريكي لا يدرس إمكانية القيام بعمليات هجومية ذكية مثل تلك التي اقترحها عليه.

كما تحدث هيدن عن إمكانية القيام بتنفيذ العمليات التي سبق أن درستها الإدارة الأميركية من أجل وقف الهجمات التي تشنها الدول الأخرى سواء تمت تلك الهجمات بموافقة تلك الدول وتمويلها أو دون معرفتها. ومن ضمن المسائل التي ناقشتها الولايات المتحدة التوقف عن التساؤل عن الجهة التي قامت بالهجوم وإمكانية العثور عليها وتحميل الدولة التي انطلق منها الهجوم المسؤولية والعمل ضدها. وقال: "إننا نأخذ بعين الاعتبار جميع أشكال المحاربة في مجال التحكم الآلي، وجميع الردود التي يمكنها أن تهدد وتمس بتدفق الإنترنت إلى الدولة التي انطلق منها الهجوم، مثل تباطؤ التدفق والمساس بمقدرة الاتصال. ومن ضمن العمليات التي تمت مناقشتها الهجوم من أجل حجب الخدمة.

ويقول هيدن: إن هذا السلاح متوفر وسهل الاستخدام، يجب علينا أن نجعل الدول تدرك أنها تتحمل المسؤولية على مجال التحكم الآلي داخلها وكل ما يحدث فيه. وتطرق إلى مجالات لا يجب المساس بها مثل شبكات الاتصالات الحساسة،ومن ضمنها شبكات الكهرباء والشبكات المصرفية. ولا شك أن في هذا تناقض غريب، لأننا في الحروب العادية تكون هذه الشبكات أهدافا مشروعة للهجوم.

سياسة الرد في مجال التحكم الآلي:

بناء على شهادة الجنرال ألكسندر أمام الكونجرس، إذا قال الرئيس الأميركي أن حادثة تحكم آلي تجاوزت الحدود على صعيد استخدام القوة، فإن من حقه أيضا أن يحدد سياسة الرد. وهذا التحديد يقوم على تقديرات خاصة وعامة، مثل الاعتماد على مواثيق الأمم المتحدة، بشأن حق الدفاع عن الذات. ومن الجدير بالذكر أنه لا توجد في الآونة الحالية قوانين متفق عليها في العالم مما يجعل بمقدور كل دولة أن تحدد لنفسها خطا أحمر خاصا تقوم بعده باللجوء لاستخدام القوة استنادا إلى القوانين الدولية التي لم تخصص لمجال التحكم الآلي بصورة خاصة.

أوروبا:

- **فرنسا:**

تدرك فرنسا الأهمية الحاسمة لمجال التحكم الآلي بالنسبة للوضع الاقتصادي، الاجتماعي والأمني والحياتي كله. وفي عام 2009 بلورت فرنسا إستراتيجية لحماية مجال التحكم الآلي، وكان هدفها على النحو التالي:

أ- أن تصبح دولة عظمى في مجال حماية منظومات المعلومات. وفرنسا تسعى للانتماء الوسط الضيق للأمم الرائدة في هذا المجال، وهي تعتزم لعب دور فعال داخل مجموعة الدول المتطورة من أجل بلورة رد مشترك للتهديدات التي يعكسها هذا المجال.

ب – إقامة مجال معلومات أمني محمي يتيح الفرصة لاتخاذ قرارات وضمان عمل أجهزة القيادة والسيطرة في حالات الطوارئ والأمان.

ج- تعزيز حماية الشبكات الحيوية والأهداف الحيوية التي تعتمد عليها. لقد حددت فرنسا قائمة للبنى الحيوية لوجود الأمة، والتي يعود قسم منها للقطاع الخاص. إن حماية هذه البنى يتطلب تأهيل القطاع الصناعي في الدولة.

د- إتاحة مجال تحكم آلي آمن. ومن أجل ذلك يجب بناء حماية من أجل مواجهة التهديدات بشن هجمات تحكم آلي ضد الجهات الحكومية، والشركات الخاصة أو المدنيين.

أساليب إنجاز الأهداف الإستراتيجية:

أ- المراقبة في ساعات شن الهجوم على فرنسا وتوفير رد سريع في حالات الهجوم.

ب- زيادة المعرفة والمقدرة العلمية في مجال التحكم الآلي بما فيها: تحسين الأبحاث حول بيئة التحكم الآلي من أجل تشخيص الاتجاهات التكنولوجية التي تخفي في طياتها تهديدات محتملة. كما سيتم

إقامة مركز أبحاث بالتعاون مع الجهات الأكاديمية والجهات الخاصة على أن يتمحور العمل حول القضايا الخاصة بالتشفير، وتحليل الهجمات وتطوير البرامج المحمية.

ج- حماية منظومات المعلومات للبنى الحيوية العائدة للدولة أو لجهات خاصة. وفي إطار هذا البند تم تحديد "الإستراتيجية القومية الفرنسية لحماية المعلومات السرية" وتشكيل شبكة إنترنت محمية للوزارات الحكومية.

د- ملاءمة التشريع مع التطورات في مجال تكنولوجيا المعلومات والشبكات.

هـ- تطوير تعاون دولي في المجال مثل حماية المعلومات ومحاربة الجرائم التي ترتكب في مجال التحكم الآلي.

و- زيادة المعرفة في هذه القضية في أوساط صانعي القرارات والجماهير الفرنسية الواسعة .

وفي إطار محاولة تجسيد الإستراتيجية المذكورة أنشئت مؤسسات على المستوى القومي، وفي إطار ذلك أنشئ المجلس الإستراتيجي لحماية منظومات المعلومات القومية التي يترأسها مدير وزارة حماية الوطن. أما أعضاء المجلس فهم: رئيس هيئة الأركان، ورؤساء الأجهزة الاستخبارية المدنيين، ومدير وزارة الخارجية، مدير وزارة الدفاع، وممثل خاص لشؤون التسليح، وشخصيات رفيعة في المجال الصناعي. إن مهمة المجلس تقوم على تفصيل الاستراتيجية القومية لحماية منظومات المعلومات وتوجيه الوكالات القومية لحمايتها.

وقد تم تنظيم وكالة حماية منظومات المعلومات ANSSI حين إقامتها عام 2009 على النحو التالي:

1- مركز عملي لحماية منظومات المعلومات COSSI على أن يعمل بصورة متواصلة ويراقب محاولات الاختراق عبر التحكم الآلي والرد بالصورة الملائمة. ويشتمل المركز على المهام التالية: مركز أبحاث تطبيقي "للتشفير، والتشخيص وإعطاء الإذن بالمرور"، مركز رقابة في مجال أمن منظومات المعلومات، مركز للرد ومعالجة هجمات التحكم الآلي، مركز متابعة، عملية تنسيق، غرفة عمليات مكتب تخطيط وتجارب.

2- شعبة إستراتيجية وضبط آلي - SR – تعمل على بلورة إستراتيجية، تحديد أنظمة، تنسيق بين الوزارات ومتابعة تقدم المجال على الصعيد العالمي.

ج- شعبة مساعدة، واستشارات وتأهيل ACE.

د- شعبة منظومات معلومات محمية، تعمل في مجال تطوير والمصادقة على وسائل الاتصالات المحمية التي سيستخدمها الكادر المهني والسياسي – على أن لا تشمل منظومات الاتصالات العسكرية.

- **ألمانيا:**

هناك العديد من السمات المتشابهة للسمات الفرنسية في الاستعدادات الألمانية لحماية مجال التحكم الآلي على المستوى القومي، بما فيها إقامة مجلس قومي ومركز عملي للردود على الهجمات التي تتعرض لها الدولة في المجال. وقد تم نشر والإعلان عن الاستراتيجية المتبعة في وثيقة "الاستراتيجية الجدية لأمن التحكم الآلي الألماني". حقا أن هذه الوثيقة تتطرق للوضع المدني، بيد أنها تشير أيضا إلى أن هناك خطوات مكملة سيقوم الجيش الألماني باتخاذها من أجل حماية إمكانياته ومن أجل حماية مجال التحكم الآلي القومي. ويبرز في هذه الوثيقة الاستراتيجية السعي نحو التعاون بين القطاع العام والخاص، والتعاون بين ألمانيا ودول ومؤسسات أجنبية. وتتطرق الوثيقة إلى القضايا التالية:

أ- الدفاع عن البنى الحساسة.

ب- تعزيز حماية شبكات المعلومات في الدولة، على سبيل المثال عبر الرقابة على مزودي الاتصالات وشركات الحماية كي لا تتورع عن اتخاذ جميع وسائل الحماية اللازمة وتقديم الحوافز اللازمة لتوفير وسائل الحماية المدنية مثل Electronic Proof of Identity .

ج- تعزيز أمن بني التحكم الآلي في الوزارات الحكومية.

د- إقامة جهاز للردود السريعة على هجمات التحكم الآلي – National Cyber Response Centre

هـ - تشكيل مجلس لبلـورة السياسـات والتنسـيق عـلى المسـتوى القـومي: National Cyber Security Council.

و- تعزيز مقدرة سلطات القانون وفرضه من أجل تحسـين مقـدرة المواجهـة مـع الجـرائم والتجسـس عـبر التحكم الآلي.

ز- تحسين التعاون والتنسيق مع الدول الأوروبية والدول الأخرى في العالم من أجل حماية مجـال الـتحكم الآلي.

حـ - استخدام وسائل أمينة من وسائل تكنولوجيا المعلومات.

ط – تأهيل عمال وتوجيه في مجال حماية شبكات المعلومات في القطاع الحكومي.

ي – إمكانية الرد على الهجمات في مجال التحكم الآلي. وقد جاء في الوثيقة: "إذا كانت الدولة ترغب في أن تكون على أهبة الاستعداد لمواجهة أي هجوم تحكم آلي. يجب خلق غطاء شامل ومتكامل من الوسائل من أجل الـرد على مثل هذه الهجمات بالتعاون مع سلطات الدولة ذات الصلاحيات.

الإستراتيجية الأمنية الصينية للتحكم الآلي:

في الوقت الذي يوجد فيه تشابه كبير بين استراتيجيات الدول الغربية بوصفها استراتيجيات دفاعية موجهـة تجاه تهديدات وأعداء مشابهين، فإن الرؤيا الصينية على هذا الصـعيد تخلـق اسـتراتيجية مختلفـة في مجـال الـتحكم الآلي، بوصفه مجال فرص يتطلب تجسيدها مقدرة على الاختراق من أجل جمع المعلومات والهجوم.

الصين تعتبر مجال التحكم الآلي مجالا استراتيجيا:

تـرى الصـين في التكنولوجيـا الرقميـة فرصـة سـانحة لتحسـين مقـدرتها الاسـتراتيجية والاقتصـادية والعسكرية ومكانتها بوصـفها دولـة عظمـى يبلـغ تعـداد سـكانها 1.35 مليـار نسـمة. وقـد تبـدى ذلـك في الانتشـار السريع جدا للإنترنت ووسائل المواصلات الخلوية في الصين. وتسعى الصين عبر التكنولوجيا المتقدمة الانتقال قفزا من مجتمـع زراعـي – حيـث يسـكن غالبيـة الصـينيين حتـى الآن في قـرى زراعيـة- إلى مجتمـع علمـي مـع التجـاوز

السريع إلى أقصى حد ممكن على مرحلة المجتمع الصناعي. يحاول الصينيون فعل ما استغرق الدول الغربية عشرات السنوات خلال فترة قصيرة بفضل التكنولوجيا الرقمية التي يتيح السوق الرقمي الصيني تجسيدها.

ويتضح من الأبحاث الأميركية التي تحلل الاستراتيجية الصينية في مجال التحكم الآلي أن عمل الصين تمحور على الصعيد الأمني منذ نهاية التسعينات وحتى الآن في مجال التحكم الآلي، والتجسس على الغرب وشن الهجمات على المعارضين السياسيين في شتى أنحاء العالم. وتقوم الصين في غضون السنوات القليلة الماضية ببناء مقدرة عسكرية للتحكم الآلي هدفها أن تتمكن من الحصول على مزايا إستراتيجية تتلاءم وكونها دولة عظمى.

والصين تعتبر أن تطور مقدرتها في مجال التحكم الآلي العسكري عاملا استراتيجيا ضروريا لموازنة تدنيها الاستراتيجي على الصعيد العسكري التقليدي مقارنة بالولايات المتحدة. ويبدو أنها تعتبر تطوير مقدرتها على هذا الصعيد بمثابة فرصة للتفوق الإستراتيجي الذي ما كانت لديها أية فرصة لنيله في الماضي. وينعكس هذا الوضع على صعيد استغلال مجال التحكم الآلي في تحسين وظائف الجيش الصيني والسعي للحصول على مقدرة هجومية تمنحها هيمنة في مجال التحكم الآلي، مما سيعكس نفسه على مجالات أخرى.

وبناء على ما تنشره مراكز الأبحاث الغربية، فإن الصين تعتبر بمثابة تهديد للغرب في ثلاثة مجالات: الأول: جمع المعلومات الذي يمكنه أن يمنحها تفوقا عسكريا، فعلى سبيل المثال كشف نقاط الضعف لدى الولايات المتحدة والمخططات العسكرية وجمع المعلومات التكنولوجية السرية العسكرية والمدنية، التي تعتبر بمثابة التفوق النوعي الأميركي، وسرقة ممتلكات التحكم الآلي – برامج وقواعد معطيات – للاستخدام العسكري والمدني.

ويعتقد خبراء في الغرب أن الصينيين يعملون بصورة أساسية ضد أهداف في الولايات المتحدة وأوروبا عبر عمليات الاختراق عن بعد عن طريق تزويد المؤسسات الأميركية والأوروبية بمعدات وتجهيزات مشفرة ومزروعة فيها برامج شريرة. لقد أفادت الأنباء عام 2009 أن هناك عملية اختراق للحواسيب الأميركية، وأن

الصين هي الفاعل، وقد سرقت خلال هذه العملية مخططات الطائرة المستقبلية المقاتلة F-35 Lightning II . كما ينسب إلى الصين اختراق حواسيب شركات تجارية مثل google من أجل جمع معلومات وشن هجمات على معارضي النظام الصيني في إطار العملية التي أطلق عليها اسم "عملية أورورە" عام 2009.

الثاني: تطوير مقدرة هجومية في مجال التحكم الآلي بصورة تهدد البنى المدنية والعسكرية المتطورة في دول الغرب. إن المقدرة التكنولوجية والعملية الصينية رفيعة المستوى جدا على صعيد جمع المعلومات يمكنها أن تشير إلى مقدرتها في مجال شن الهجمات.

الثالث: الصراع الحضاري: تحدي الصين لقيم الغرب مثلما تحاول الولايات المتحدة تطبيقها في مجال التحكم الآلي العالمي، مثل حرية المعلومات وحماية حقوق الملكية الروحانية. ويذكر أنه وفي أعقاب قيام القراصنة الصينيون بشن هجمات على الولايات المتحدة، والأزمة التي نشبت بين الصين و"google"، وجهت وزيرة الخارجية الأميركية هيلاري كلينتون في الثاني عشر من كانون الثاني 2010 تحذيرا يفيد إن الولايات المتحدة ستدافع عن شبكاتها، وأن كل من يحاول المساس بها أو يهدد المجتمع الأميركي المدني والاقتصاد الأميركي سوف يتحمل النتائج ويحظى بشجب دولي.

خصائص الاستعدادات التي تقوم بها الدول للعمل في مجال التحكم الآلي:

لم تكن الدول حتى السنوات القليلة الماضية في حاجة لإقامة أجهزة أو منظومات خاصة لإدارة الحرب في مجال التحكم الآلي، باستثناء إقامة سلطات لحماية المعلومات، ويبدو أن الجيوش ومنظمات المخابرات ووزارات الأمن الداخلي ألموا في تطبيق هذه النشاطات عبر إنشاء جهات عملية داخل الوحدات التابعة لها. إن الأحداث التي وقعت في غضون السنوات الأخيرة وإدراك الأخطار القائمة والفرص السانحة في مجال ميادين قتال التحكم الآلي غيرت الصورة وأشارت إلى ضرورة العمل على إعادة التنظيم من جديد، وهو الأمر الذي يبدو لدى العديد من الدول.

- الانتقال من اتجاه حماية المعلومات إلى نظرية الدفاع: أقامت العديد من الدول في مطلع الألفين جهات قومية لحماية شبكات ومنظومات المعلومات، والتي كانت في أصلها جهات حماية معلومات. وفي نهاية العقد طرأ تطور تنظيمي يتلاءم وكون مجال التحكم الآلي هو مجال قتال، لذا تمت بلورة إستراتيجيات دفاعية عن المجال القومي الالكتروني. إن الرد التنظيمي على تحدي التحكم الآلي في العديد من الدول يتألف من طابقين:

أ- يوجد في الطابق الأعلى الكادر السياسي الأعلى والذي يدير جهة على مستوى وزارة حكومية – في الولايات المتحدة وبريطانيا، أو مجلس قومي – في فرنسا وألمانيا. وعلى هذا المستوى يعكفون على بلورة إستراتيجية وقواعد سياسية، والملاءمة بين جميع العناصر العاملة في الدولة في مجال حماية مجال التحكم الآلي.

ب- وفي الطابق الثاني تعمل وحدات أو منظمات أمنية عسكرية – مثل قيادة التحكم الآلي في الولايات المتحدة- ومدنية – مثل قسم أمن التحكم الآلي في وزارة أمن الوطن في الولايات المتحدة.

هناك فارق بين الاستعدادات الدفاعية التي تشمل جميع القطاعات وبين مجال الهجوم القائم كله في مجال المؤسسات العسكرية وجماعات المخابرات – مثل وزارة الدفاع الأميركية ووكالة المخابرات المركزية. ويبدو أن قرار بناء المقدرة الهجومية وتفعيلها يتخذ ضمن سلسلة القيادات المباشرة القائمة بين الجهات الأمنية المذكورة والجهات المسؤولة عن التحكم الآلي. وتشمل سلسلة القيادة الأميركية الرئيس ووزير الدفاع وقائد القيادة الإستراتيجية وقائد قيادة التحكم الآلي، ولا تعمل عبر جهات مدنية مثل وزارة أمن الوطن.

-الدمج العملي بين الجهات المدنية والعسكرية: إن إدراك كون مجال التحكم الآلي مشترك بين القطاعين الأمني والمدني يعتبر بمثابة محرك للقيام بعمليات تنظيم عملية مشتركة. وليس أدل على ذلك من إقامة "مراكز العمليات" المشتركة، مثلما هو حادث في بريطانيا، فرنسا وألمانيا. والتي تضع نصب عينيها هدف تجميع صورة الوضع وتقديم المساعدة حين الحاجة. ورغم ذلك فإن هناك عملية تقسيم عمل واضحة جدا بين

القطاعات المختلفة في هذه الدول الديمقراطية وفي الولايات المتحدة. فالجهات المدنية تعتبر مسؤولة عـن العمليـات الدفاعية داخل الدولة، في حين أن الجيوش والأجهزة الاستخبارية - التي تتمتع بمقدرة هجومية- تـدافع عـن نفسـها، وتزود المدافعين بمعلومات حول الأعداء والخصوم، وتساعد الوحدات المدنية في الدفاع عن البنى الحيوية - وخصوصا في حالات الطوارئ التي تزداد خلالها صلاحيات الجيوش، وتوجه تواجدها ومقدرتها الهجومية في مجـال الـتحكم الآلي لإسكات مصادر الهجوم، والرد عليها بالصورة المناسبة.

إن السعي للتعاون في مجال التحكم الآلي مع الدول الصديقة هو معيار بـارز مـن معـايير الإسـتراتيجية في الدول الغربية.

الفصل الرابع

المغزى التنظيمي الإسرائيلي

- الاقتصاد الإسرائيلي يستند إلى حد كبير على بنى مجال التحكم الآلي وأفرع تكنولوجيا المعلومات تسهم إسهاما مباشرا وغير مباشر في نمو الاقتصاد الإسرائيلي.

- يسهم اقتصاد الانترنت في إسرائيل إسهاما كبيرا أيضا في خلق أماكن عمل وخصوصا للأكاديميين في مجال التكنولوجيا وتسهم أفرع تكنولوجيا المعلومات إسهاما مباشراً وغير مباشر في دعم القطاعات الأمنية .

- إن مجال التحكم الآلي يمكن إسرائيل من كسر عزلتها الجغرافية في الشرق الأوسط وإقامة علاقات وطيدة وشاملة مع العالم.

- هيئة التحكم الآلي العسكرية قادرة على أن تكون شريكا في حماية مجال التحكم الآلي في إسرائيل بيد أنها ليست الجهة الخاصة والقومية لحماية مجال التحكم الآلي القومي.

أهمية تكنولوجيا المعلومات ومجال التحكم الآلي بالنسبة لإسرائيل:

تسهم تكنولوجيا المعلومات ومجال التحكم الآلي إسهاما إستراتيجيا في بناء إسرائيل. فالاقتصاد الإسرائيلي – وعلى غرار ما هو سائد في الدول المتقدمة في العالم – يستند إلى حد كبير على بنى مجال التحكم الآلي. وأفرع تكنولوجيا المعلومات تسهم إسهاما مباشرا وغير مباشر في نمو الاقتصاد الإسرائيلي. هذا وتعتبر إسرائيل من بين الدول الرائدة في العالم في تطوير تكنولوجية المعلومات.

وتفيد أبحاث شركة الاستشارات الدولية مكنزي إن اقتصاد الإنترنت في إسرائيل ينقسم إلى مجالين: وأن القسم الأعظم منها يأتي في مجال صناعة تكنولوجيا المعلومات والاتصالات ICT والذي يتضمن التطوير، الإنتاج، بيع التجهيزات، والبرامج والخدمات. أما المجال الثاني الأصغر والذي ينمو بسرعة فهو مجال التجارة الالكترونية والذي يعمل في مجال اكتساب منتجات وخدمات على الانترنت.

وبناء على البحث فإن اقتصاد الانترنت في إسرائيل - بناء على تقديرات مكنزي أسهمت في الناتج الوطني الخام بصورة مباشرة بمبلغ خمسين مليار شيكل عام 2009 –حوالي 6.5% من الناتج المحلي الخام. ولا شك أن هذه المعطيات تضع إسرائيل في مصافي إحدى اقتصاديات الإنترنت الرائدة في العالم. ويتوقع البحث أن ينمو اقتصاد الإنترنت في إسرائيل بوتيرة سنوية نسبتها 9% - أي ضعف وتيرة نمو الاقتصاد الإسرائيلي. ومن المتوقع أن يبلغ حجم مساهمة اقتصاد الانترنت الإسرائيلي عام 2015 مبلغ 85 مليار شيكل، أي 8.5% من قيمة الناتج الوطني الإسرائيلي الخام.

هناك أهمية خاصة لشعبة تكنولوجيا المعلومات نظرا لمقدرتها العالية على المنافسة في السوق العالمي – قسم كبير من الناتج يوجه إلى الخارج- ونظرا لأن الطريقة الوحيدة لإسرائيل كي تنمو بسرعة هي زيادة حجم الصادرات.

ويسهم اقتصاد الانترنت إسهاما كبيرا أيضا في خلق أماكن عمل، وخصوصا للأكاديميين في مجال التكنولوجيا. كما تسهم أفرع تكنولوجيا المعلومات إسهاما مباشراً وغير مباشر في دعم القطاعات الأمنية في

إسرائيل. إن أفرع تكنولوجيا المعلومات هي جزء هام من مقدرة التكنولوجيا الإسرائيلية والتـي تحظـى بـالكثير مـن التقدير من الخبراء في شتى أنحاء العالم، مما يعزز مكانة إسرائيل في العالم.

إن مجال التحكم الآلي يمكن إسرائيل من كسر عزلتها الجغرافية في الشرق الأوسط وإقامة علاقـات وطيـدة وشاملة مع العالم. كما أن هناك، في هذا المجال، فرصا لتعزيز الصلة بين الضواحي والمناطق المدنيـة في الدولـة، وهـي تلعب دورا مركزيا في العمل الاجتماعي، وفي تعزيز الصلة بين السلطات والمواطن.

الاستعدادات الإسرائيلية لحماية مجال التحكم الآلي:

يمكننا الإشارة في إطار الاستعدادات التي تتخذها إسرائيل لحماية مجال التحكم الآلي الخاص بهـا إلى عـدة نقاط هامة. ففي عام 1997 أنشأت هيئة "تهيله" – الهيئة الحكومية لعهـد الإنترنـت- وقـد أنشـئت هـذه الهيئـة في مكتب المحاسب العام في وزارة المالية،وهو يرمي لتقديم خـدمات دخـول مؤمنـة إلى الإنترنـت لـوزارات ومؤسسـات الحكومة. وتقوم هذه الهيئة بتزويد مئات الإسرائيليين وغير الإسرائيليين بخدمة دخول المواقـع الوزاريـة والمؤسسـات الحكومية الإسرائيلية على الانترنت. وهي تستخدم العديد من الوسائل للحفاظ على أمن المؤسسات الحكوميـة، بـدءا من استخدام طاقم خبراء لحماية المعلومات والاتصالات وانتهاء بمنتجات ومعدات تكنولوجيـة مـن شركـات رائـدة في العالم.

وقد أقامت هذه الهيئة مركز حماية معلومات للحكومة الإسرائيلية، والذي من بين وظائفه متابعة عمليـة حماية المعلومات في العالم مع الانتبـاه إلى الهجـمات التـي تشـن عـلى الانترنـت وخصوصـا التـي تسـتهدف إسرائيـل، والتنسيق بين الجهات الحكومية من أجل حل مشاكل الحمايـة، والـربط بـين الجهـات الحكوميـة والجهـات الأجنبيـة وإجراء الأبحاث في هذا المجال.

ويصـدر المركـز تحـذيرات حمايـة معلومـات للمـنظمات في مجـال تكنولوجيـا المعلومـات للجهـات التي تجري اتصالات مع "تهيله" أو الجهات الحكومية غر المصـنفة سريـا. كـما يجـري المركـز اتصـالات مـع الجهـات الدوليـة مـن أجـل القضـاء عـلى الهجـمات المحوسـبة. ويعمـل في إطـار ذلـك طـاقم يسـمى " CERT: Computer

Emerge4ncy Response Team " والـذي يعمـل في مجـال تـوفير الـرد المناسـب لأحـداث الحمايـة في المـنظمات الحكومية أو الجهات الدولية بصورة فورية. ويعمل ممثلو الطاقم على إقامة قسم لمواجهة الهجمات التي تشـن عـبر الشبكات، وإدارة المخاطر، وخلق إجراءات حماية معلومات، الرقابـة عـلى الاتصـالات واختراقـات الفيروسـات، ومنـع البريد القذر، وأعمال القرصنة في الشبكات،وتزوير الهويات، والحفاظ على خصوصية المعلومات، ورفـع مسـتوى فهـم الحمايـة، وكـذلك يعمـل في مجـال التعـاون وإطـلاع شركـات الإنترنـت، والشرطـة والجهـات الأمنيـة عـلى المعلومـات الضرورية. لقد أخذ هذا المركز على عاتقه مهمة صعبة للغاية، بيد أنه يتوجب أن نتذكر أن مهمتـه تقـوم عـلى تـأمين حماية كاملة للوزارات الحكومية الإسرائيلية للدخول إلى الانترنت.

وفي السابع والعشرين مـن آذار 2011 صـادقت الحكومـة عـلى إقامـة وحـدة "النمـر" - إدارة منظومـات المعلومات- الحكومية،وهي جهة وزارية ستعمل على تركيز مجال الحاسوب والاتصالات في الحكومة. ومـن المفـروض أن يوجه هذا المركز الخاضع لمدير عام وزارة المالية وحدات الحاسوب والاتصالات في الـوزارات الحكوميـة وأن يكـون مسؤولا بصورة مباشرة عن كل مشروع الحوسبة الحكومية بما فيها عن مشروع "تهيلـه". إن تركيـز مشروع الحوسـبة الحكومية في مكان واحد يعتبر بمثابة تقدم كبير في اسـتعدادات الدولـة في مجـال الحوسـبة والاتصـالات، بيـد أن مـن الأفضل أن تكون الجهة المسؤولة عن إدارة أمـن منظومـات المعلومـات مـن خـارج هـذه الإدارة التـي تقـوم بإنشـاء وتفعيل تلك البنى.

وفي عام 2002 تم إنشاء السلطة الحكومية لحماية المعلومات في جهاز الأمن العام، والتـي تعتـبر مسـؤولة عن التوجيه المهني للجهات الواقعة تحت مسؤوليتها في مجال حماية بنى الحوسبة الحيوية من التهديدات الإرهابيـة والتخريبية في مجال حماية المعلومات المصنفة سرية، ومن تهديدات التجسس وكشف المعلومات. إن المنطـق القـائم خلف وجود هيئة واحدة مسؤولة في جهاز الأمـن العـام يقـوم عـلى أن الجهـاز هـو المسـؤول عـن كشـف عمليـات التجسس والإرهاب.

ويمكننا أن نشير إلى العديد من المزايا والعيوب لهذه الطريقة، وأول هذه المزايا يتمثل في العلاقة الوطيدة بين الشبكة وبين باقي صلاحيات وقدرات جهاز الأمن العام، وجماعة الاستخبارات التي يشارك الجهاز فيها. ومن الناحية الأخرى قد تتردد جهات في القطاع الخاص من كشف نفسها أمام وحدة هذا الجهاز الذي يتولى مهام ويمتلك صلاحيات غير عادية لا تتعلق فقط بهذا المجال. هذا عداك عن كون جهاز الأمن العام بطبيعته هو جهة عملية تعمل في مجال عمليات الإحباط السرية، ولا تقوم بأية مهام مطلوبة من أجل مواجهة تحديات التحكم الآلي، مثل إقامة علاقات وطيدة مع القطاعات الخاصة، تعزيز المعرفة الجماهيرية لحماية التحكم الآلي، معالجة الجهات المتضررة جراء هجمات التحكم الآلي وغيره.

وتقوم لجنة توجيه حماية منظومات الحوسبة في هيئة الأمن القومي بتوجيه السلطة الحكومية لحماية المعلومات في جهاز الأمن العام. ومن مهام هذه اللجنة المصادقة على قيام سلطة حماية المعلومات بتوسيع قائمة الجهات التي تحتاج إلى التوجيه أو الحماية، أو التي تحتاج إلى تعميق حمايتها. وبناء على المقالة التي كتبها جابي سيبوني فإن هذه العمليات لم تقم على مسارات إجرائية ومنهجية للعثور على هذه الجهات والمصادقة عليها، الأمر الذي جعل القائمة تشتمل على أسماء شركات كبيرة وحيوية في قطاعات معينة في حين أن شركات كبيرة وحيوية في قطاعات أخرى لم تشملها رغم أن مساهمتها في الناتج الوطني الخام والتشغيل وباقي مناحي الحياة في إسرائيل كبيرة.

وهناك عيب آخر في هذه الطريقة يتمثل بأنها تركز على توجيه شركات مختارة في قطاعات معينة، مما يسهم في مساعدة وحماية موضعية وليست حماية شمولية لتلك الجهات. وأبرز نموذج على ذلك شبكة المياه: إن حماية شبكات المياه ونوعيتها في إسرائيل لا تتعلق فقط بالإجراءات القائمة في شركة "مكوروت" التي يظهر اسمها في القائمة، بل يتعلق أيضا بعشرات مزودي المياه الآخرين:روابط، اتحادات مياه، منشآت تحلية، ونقل، منشآت معالجة مياه المجاري ، منشآت معالجة ونقل المياه غير الصالحة وغيره. إن القسم الأكبر من هذه المنشآت يتم تشغيله عن طريق مبادرين خاصين، والذين لا يضعون مسألة الحماية على رأس جداول أعمالهم.

هيئة التحكم الآلي العسكرية:

لقد وصف رئيس الأركان جابي أشكنازي عام 2009 مجال التحكم الآلي بأنه مجال حرب إستراتيجي وعملي، وبناء على ذلك تم إنشاء هيئة التحكم الآلي العسكرية والتي أعدت كي تقوم بدور هيئة أركان لتنسيق وإعداد العمليات العسكرية في مجال التحكم الآلي. وقد أقيمت الهيئة في الوحدة 8200 من شعبة الاستخبارات العسكرية، وقد شارك فيه ممثلون عن شعبة الاستخبارات العسكرية وشعبة الاتصالات والحوسبة. وقد تطرق اللواء عاموس يادلين بوصفه قائدا لشعبة الاستخبارات إلى هذه القضية في المحاضرة التي ألقاها في معهد أبحاث الأمن القومي في كانون الأول 2009، وأشار خلالها إلى الاحتمالات القائمة للمساس بإسرائيل جراء اقتحام أحد الحواسيب بوصفها تهديدا قوميا. وقال: "يعتزم الجيش الإسرائيلي توفير حماية جيدة للشبكات، وتفعيل هجمات تحكم آلي". إن هيئة التحكم الآلي العسكرية قادرة على أن تكون شريكا في حماية مجال التحكم الآلي في الدولة، على غرار قيادة التحكم الآلي في الولايات المتحدة، بيد أنها ليست الجهة الخاصة والقومية لحماية مجال التحكم الآلي القومي.

هيئة التحكم الآلي القومية:

أعلن رئيس الحكومة نتنياهو في الثامن عشر من أيار 2011 عن تشكيل هيئة التحكم الآلي القومية، وبناء على بيان مكتب رئيس الحكومة فقد جاء فيه: "إن الهدف الرئيس من هذه الهيئة هو توسيع مقدرة الحماية التي تقدمها الدولة لمنظومات البنى التحتية الحيوية ضد هجمات إرهاب التحكم الآلي، التي يجري تنفيذها على أيدي الدول الأجنبية أو الجهات الإرهابية.

لقد تم إنشاء هذه الهيئة في أعقاب التوصيات التي قدمها رئيس مجلس الأمن القومي للأبحاث والتطوير اللواء اسحق بن يسرائيل. وقد أعلن نتنياهو أنه تبنى التوصيات بكاملها وأوضح ذلك بالقول: "على الصعيد الدفاعي، إسرائيل معرضة لهجمات تحكم آلي قادرة على شل منظومات حياتية تقوم بتشغيل الدولة

مثل: الكهرباء، والاتصالات، وبطاقات الاعتماد، والمياه، والمواصلات. إن جميع المجالات المحوسبة معرضة للأضرار. لذا هناك ضرورة لبلورة ردود دفاعية لهذه التهديدات".

وأفادت الأنباء أن من المتوقع أن تعمل الهيئة الجديدة على تبني شركات إسرائيلية متخصصة في مجال الحماية عن مجال التحكم الآلي في محاولة للحصول على قسم من هذا المجال الآخذ في التطور في السوق العالمي.

إن إقامة هذه الهيئة سيعتبر بمثابة تجديد كبير، نظرا لأنه وحتى الآن لا يوجد في إسرائيل جهة تشرف على حماية مجال التحكم الآلي وفقا لرؤيا قومية. لقد تمحورت المعالجة الدفاعية لمجال التحكم الآلي في إسرائيل حول الوحدات العملية – في وزارة المالية، جهاز الأمن العام والجيش- وهو الأمر الذي افتقر إليه الكادر السياسي والإستراتيجي الأعلى.

توصيات لإسرائيل

هناك ثلاثة أسباب رئيسية لإسرائيل تدفعها لتسريع استعداداتها الأمنية في مجال التحكم الآلي:

أ- على غرار الدول الغربية المتطورة الأخرى، فإن مجال التحكم الآلي يعرض إسرائيل لأخطار جذرية كبيرة، ومن ضمنها أخطار يمكنها أن تمس بالبنى الحيوية، والأجهزة الأمنية ووظائف الاقتصاد وغيره.

ب- على عكس العديد من الدول، فإن إسرائيل تواجه أعداء لديهم محفزات واضحة ومعلنة للقضاء عليها إذا استطاعوا ذلك، مثل إيران التي تعمل من أجل الحصول على مقدرة تحكم آلي هجومية. ومن الجائز أيضا شروع المنظمات الإرهابية بعمليات هجومية في مجال التحكم الآلي ضد إسرائيل.

ج- بمقدور إسرائيل – التي تعتبر من بين الدول الرائدة في مجال تكنولوجيا المعلومات والتحكم الآلي- تطوير مقدرة دفاعية متقدمة واستنفاد المزايا التي يمنحها إياها التحكم الآلي في ساحات القتال.

إن إسرائيل في حاجة في إطار العمل على تسريع استعداداتها للقيام بالخطوات التالية:

1- ترسيم إستراتيجية قومية لأمن مجال التحكم الآلي الإسرائيلي وتطبيق الإستراتيجية على صعيد إدارة هيئة التحكم الآلي القومية.

2- إدراج حرب التحكم الآلي بوصفها مركبا في إستراتيجية الأمن الإسرائيلية.

إن الإعلان عن إنشاء هيئة التحكم الآلي القومية هي حقا خطوة هامة أخرى في المواجهة الإسرائيلية لتحديات التحكم الآلي، بيد أنه يجب ضمان أن تعمل هذه الهيئة وفقا لإستراتيجية تحكم آلي قومية يتم بلورتها لذلك. وإزاء تخلف إسرائيل على هذا الصعيد، فإن من المهم أن يتم إنشاء الهيئة بسرعة وأن تتحمل مسؤولياتها وتمنح الصلاحيات اللازمة كي تتمكن من سد الثغرات القائمة على المستوى القومي فيما يتعلق بإدارة إستراتيجية وتوحيد لجميع الجهات العملية – المدنية والعسكرية- العاملة في مجال التحكم الآلي والمجال الدفاعي.

إستراتيجية حماية مجال التحكم الآلي في إسرائيل : اقتراحات:

نقترح على إسرائيل أن تبلور إستراتيجية قومية لأمن مجال التحكم الآلي تفضي لتحقيق الأهداف الإستراتيجية باستخدام الحد الأدنى من الموارد، وتعمل كإطار لعمل جميع الجهات المشاركة في حماية مجال التحكم الآلي. ويجب أن يصادق المجلس الوزاري على الإستراتيجية وعلى أن تستخدم كخط توجيه للعمل المشترك من قبل الجهات المختلفة ولعمل كل جهة على حدى. ونورد فيما يلي الأهداف الإستراتيجية ومبادئ عملها العامة:

أهداف الإستراتيجية:

أ- إنشاء مجال تحكم آلي آمن في إسرائيل يتيح للدولة فرصة تجسيد أهدافها القومية في مجال الحكم، الأمن، الاقتصاد، المجتمع، الخارجية العلوم وغيره.

ب- تعزيز أمن مجال التحكم الآلي الإسرائيلي والحفاظ على حرية العمل فيه لصالح الجماهير كلها.

ومن المفروض أن تعمل الإستراتيجية على تحسين إمكانية إنجاز الأهداف عبر الدمج بين قوى جميع الجهات ذات العلاقة في الدولة، وفقا لمبادئ العمل التالية:

1- الاعتراف بمجال التحكم الآلي بوصفه مجالا قوميا جديدا يجب الدفاع عنه بصورة خاصة – وذلك على عكس المجالات العسكرية التقليدية- من خلال رؤيا شمولية وتعاون بين جميع الجهات ذات العلاقة بالأمر.

2- تشكيل زعامة وجهاز مركزي لحماية مال التحكم الآلي على المستوى القومي .

3- إدارة الأخطار من خلال رؤيا شاملة بما في ذلك وضع البنى القومية الحساسة والأجهزة الأمنية على رأس سلم الأولويات، إضافة إلى حماية أجهزة أخرى في الاقتصاد والمجتمع الإسرائيلي، مثل حماية بنوك المعلومات في الجامعات ومراكز الأبحاث، وحماية الشركات ذات التأثير على الاقتصاد والتي لا تدخل في إطار مفهوم البنى التحتية، حماية الشركات ذات العلاقة بالبنى الحيوية وغيرها.

4- بناء جهاز دفاعي ديناميكي موحد وشامل ومن ضمنه: الدمج بين المنظومات الدفاعية السلبية وبين منظومات الدفاع الفعالة. الدمج بين حماية الأهداف الحيوية وبين عوامل الحماية القطرية – المواصلات القادمة إلى الدولة، والاتصالات- تحسين هندسة الشبكات، توطيد الروابط بين أجهزة الحماية المادية وأجهزة حماية التحكم الآلي.

5- الدمج بين القوات في القطاعات العامة – الحكومية- بين القطاع الأمني وبين القطاع المدني، وأيضا التعاون وتأطير الجهود بين الوحدات داخل كل قطاع من تلك القطاعات. فعلى سبيل المثال تأطير الجهود والمشاركة في المعلومات بين الجيش وقوات الأمن الأخرى.

6- تعاون وطيد بين القطاع الحكومي – الأمني والمدني- وبين القطاع الخاص في الدفاع عن مجال التحكم الآلي بما فيها المشاركة في المعلومات والمقدرة، بحيث أن كل منظمة حكومية وخاصة تكون على علم بالأخطار، وأحداث الهجوم وإمكانيات الدفاع الحديثة.

7- تعاون وطيد مع الجهات الخارجية. مثل بناء منظومات مراقبة شاملة مع الدول الحليفة.

8- بناء تشريع وفرض قوانين بصورة تتيح الفرصة للقيام بعمليات دفاعية .

9- مساعدات للجماهير في الدفاع عن مجال التحكم الآلي. كالقيام بعمليات إعلامية لزيادة معرفة الجماهير بالتهديدات والحلول، تقديم محفزات للأعمال ولشراء برامج الحماية، زيادة الرقابة على شركات الحماية ومزودي الاتصالات للجماهير .

10 بناء مقدرة للتخلص من نتائج الهجوم بسرعة .

11- استخدام وسائل وأساليب تكنولوجية متقدمة.

12- بلورة سياسة ردع، إحباط هجمات ورد كعوامل مكملة للإستراتيجية، بما فيها: إمكانية الرد المباشر ضد أجهزة التحكم الآلي المهاجمة، وإلحاق الأضرار بها.

وإذا أردنا تطبيق هذه الإستراتيجية فإننا نقترح أن ندرج ضمن مهام هيئة التحكم الآلي القومية الوظائف التالية:

أ- تقديم المساعدة للكادر السياسي في اتخاذ القرارات وبلورة السياسات في مجال حماية مجال التحكم الآلي القومي، بما فيها بلورة اقتراحات لبناء إستراتيجية قومية لحماية المجال بالتعاون مع الجهات ذات العلاقة والتي يصادق عليها المجلس الوزاري المصغر.

ب- تقدير الأخطار بصورة شاملة وبالتوقيت المناسب بالاعتماد على المعطيات والتقديرات الكافية للجهات الاستخبارية والعملية والتكنولوجية ذات العلاقة.

ج- تقديرات وضع بصورة شاملة وبالتوقيت المناسب، وتقديم توصيات للعمل بناء على التحليلات والبدائل.

د- توجيه أوامر وفقا للإستراتيجية إلى الجهات المدنية المشاركة في الحماية عن مجال التحكم الآلي والتنسيق مع الجهات في القطاع الأمني.

هـ - تنسيق عمليات جميع الجهات الحكومية والخاصة ذات العلاقة بـأمن مجـال الـتحكم الآلي، بمـا فيهـا تحميل المسؤولية للوزارات الحكومية المدنية من أجل العمل على تحسين أمن مجال التحكم الآلي كل في مجالها.

و- إقامة مركز عملي سياسي – مركز عمليات تحكم آلي- وإدارته على أن تتمثل مهمته في خلق صورة وضع ديناميكي للتهديدات على المجال، والتعاون في مجال المعلومات مع جميـع الجهـات ذات العلاقـة والمسـاعدة في إدارة عملية الدفاع.

ز- التعاون مع الدول الأخرى في هذا المجال.

ح- الرقابة على تنفيذ وتجسيد الإستراتيجية في هذا المجال، التأكد من وجود الرقابة اللازمة عـلى الـوزارات والمؤسسات الحكومية المختلفة والسلطات المدنية، ومراقبة والإشراف على مزودي الانترنت، وخصوصا التجهيزات التي يستخدمونها وتطبيق مبادئ السلامة العامة لأمن التحكم الآلي.

إدراج مجال التحكم الآلي في إستراتيجية إسرائيل الأمنية:

إن إضافة ميدان معارك جديد إلى ميادين الحرب الأربعة المعروفة – البرية والبحرية والجوية والفضـائية- يتطلب إدراج مجال التحكم الآلي في إستراتيجية الأمن الإسرائيلية ونظرياتها الأمنية. لقد قامت لجنة برئاسـة الـوزير دان مريدور والتي كلفها وزير الدفاع الإسرائيلي عمير بيرتس بإعداد اقتراحـات جديـدة لنظريـة الأمـن الإسرائيليـة في نيسان 2006. وقد أشارت اللجنة إلى العلاقة الضعيفة لمصطلح الردع بالنسبة لمحاربة الإرهاب، والصعوبات الناجمـة عن تطبيق مصطلح الحسم، واقترحت إضافة مصطلح دفـاعي إلى عوامـل نظريـة الأمـن الإسرائيليـة الثلاثـة – الـردع، الحسم والتحذير.

لقـد قـال اللـواء عـاموس يـادلين بوصـفه رئـيس شـعبة الاسـتخبارات العسـكرية في كـانون الأول 2009: إن مجال حرب التحكم الآلي يتناسب تماما مع النظريـة الهجوميـة الإسرائيليـة. إن هـذا المجـال هـو مجـال إسرائـيلي

بحث ولا يعتمد أبدا على أية مساعدات تكنولوجية أجنبية، خصوصا وأن الشبيبة الإسرائيلية تعرف هذا المجال جيدا، بل لقد وصفت إسرائيل في الآونة الأخيرة بأنها دولة مشروعات وبرامج الانترنت.

الفصل الخامس

الاستخدام الإستراتيجي لحرب

التحكم الآلي في المواجهات

- لان إسرائيل لم يسبق أن أعلنت أن بحوزتها أسلحة نووية فإن من حق الدول الأخرى أن تتظاهر بأن إسرائيل لم "تتجاوز الحد " في المجال النووي.

- الولايات المتحدة تستخدم سياسة الغموض "بخصوص طائرات "بردتور" وصواريخ ملاحية من أجل اغتيال أعضاء القاعدة في دول كاليمن وباكستان.

- ليس بمقدور حرب التحكم الآلي أن تقتل وحدها شخصا أو تدمير أكثر مما ينبغي ولا يمكنها أن تحتل أراض أو تغير نظاما.

- هجمات التحكم الآلي التي تستخدم بدلا من الأساليب المتحركة المعروفة تخلق غموضا كبيرا جدا على صعيد النتائج والمصادر والأسباب.

- مجال حرب التحكم الآلي الذي من المحتمل أن تدخل إليه المنظمات الإرهابية يحمل في أحشائه احتمالات التغيير في موازين القوى في المجتمع، نظرا للقوة التي يمنحها للمهاجمين.

تحتفظ البديهيات السياسية بمكانة هامة ومحترمة للغموض الإستراتيجي. إن عدم استعداد الدول بصورة مقصودة للإعلان عن الأعمال التي تقوم بها – أو ما تعتزم فعله- إلى جانب عدم وجود أية أدلة تثبت أنها فعلت أو ستفعل يعفي الدول من المسؤولية، فهي في هذه الحالة قادرة على الادعاء بأن جهة ما قد فعلت ما فعلت، لكن إذا كانت احتياجاتها تتطلب منها فعل ذلك، فيمكنها التظاهر بأن شيئا لم يحدث. أي أن بالإمكان تغيير مستويات الشكوكية: من شك مطلق – بحيث لا تعرف أية جهة ما حدث، أو ما الذي سيحدث- إلى حالة شك صغيرة جدا. ورغم ذلك يكون المنفذون في جميع الحالات قد وفروا مبررا للدول الأخرى لتبني ما فعلوا.

نماذج للغموض الإستراتيجي في المجال المادي:

إن أحد النماذج القديمة والمعروفة منذ سنوات طويلة ويحتفظون لها بمكانة خاصة، هي رفض إسرائيل الاعتراف أو النفي بأن بحوزتها أسلحة نووية. ولا شك أننا لن نجد محللا واحدا يستحق الاحترام يؤمن بأن إسرائيل لا تمتلك أسلحة نووية. لكن ونظرا لان إسرائيل لم يسبق أن أعلنت أن بحوزتها أسلحة نووية، فإن من حق الدول الأخرى أن تتظاهر بأن إسرائيل لم "تتجاوز الحد " في المجال النووي. ولا شك أن هذا الوضع مريح للدول الواقعة تحت ضغط من شعوبها للرد بوضع برامج نووية خاصة بها إذا بدت مكانة إسرائيل على هذا الصعيد جلية للعيان. كما أن هذا الوضع يساعد الدول التي لا تستطيع تصدير منتجات معينة لإسرائيل لو كان وضعها النووي علنيا. وفي نفس الوقت لا تقوم أية دولة بالتعامل مع إسرائيل على أساس أنها لا تملك أسلحة نووية.

وهناك غموض مماثل تلجأ إليه الولايات المتحدة في استخدام "طائرات صغيرة دون طيار" من نوع "بردتور" وصواريخ ملاحية من أجل اغتيال أعضاء القاعدة في دول كاليمن وباكستان. وتقوم السياسة الأميركية على نفي وجود مثل هذه الطائرات أو الصواريخ. بل إن الزعيم اليمني زعم أن هذه العمليات هي عمليات يمنية، وهو الأمر الذي بدا غير منطقي، ولم يقبله سوى قلة من المحللين. وحتى وقتنا هذا لم تعترف الدول المذكورة بالاعتداءات التي وقعت على أراضيها، مما جنبها مواجهة مشكلة انتهاك سيادتها.

أما النموذج الآخر الذي يمكننا أن نتطرق إليه فهو سياسة الولايات المتحدة تجاه استقلال تايوان. لقد أعلنت الولايات المتحدة أنها تعارض الإعلان عن استقلال تايوان وتعارض أية محاولة لتسوية مشكلة تايوان بالقوة. والولايات المتحدة لا تعترف بتايوان كدولة، وبناء على ذلك لم تعقد معها أية اتفاقيات مساعدات متبادلة، لذا فإن السؤال الذي يطرح نفسه هو: إذا أعلنت تايوان عن الاستقلال وقررت الصين احتلالها، هل ستتدخل الولايات المتحدة لصالح تايوان؟ من الواضح أن مصالح الولايات المتحدة تقتضي أن تعتقد الصين أن هذا ما سيحدث فعلا كي لا تبدأ الحرب، كما أن من مصلحة الولايات المتحدة أن تفكر تايوان بأن الوضع سيكون فعلا على هذا النحو كي لا تشجع هي الصين للشروع بشن الحرب. دعنا نفترض أن التدخل الأميركي مثله كمثل الرهان على وجه عملة حين إلقائها إلى الأرض، وفي هذه الحالة فإن تايوان ستصل إلى استنتاج مفاده أن القيمة المرتقبة من الإعلان عن الاستقلال سلبية نظرا لأن الولايات المتحدة قد لا تتدخل. وكذلك الصين ولأسبابها الخاصة قد تصل إلى نفس الاستنتاج، أي أن شن الحرب واجتياز المضائق سيكون سلبيا نظرا لأن الولايات المتحدة قد تتدخل. ولا شك أن أي موقف غموض أقل من هذا الوضع يمكنه أن يدفع هذه الدولة أو تلك لاتخاذ موقف متسرع.

مجال التحكم الآلي ملائم للغموض:

حرب التحكم الآلي هي بطبيعتها حرب سرية،فعندما يقتحم مخترقو الحواسيب منظومة حاسوب من أجل تشويش عملها، فإن النتائج المباشرة في الغالب لا تكون مرئية أمام العالم الخارجي. وبناء على درجة التشويش والتخريب في المنظومة فإن النتائج غير المباشرة لا تكون مرئية للعيان. إن هجوم التحكم الآلي الذي قد يشن على شبكة كهرباء بصورة تطفئ الأنوار، يمكن رؤيتها حتى من الفضاء، لكن عدم مواصلة التحقيق ومحاولات الاكتشاف فلن نعرف فيما إذا كانت عملية التعتيم هي نتاج للهجوم الموجه أو ناجمة عن خطأ إنساني، أو برنامج فيه عيب ما وأحيانا تفعل الطبيعة فعلها. وإذا اتضح أن منظومة ما تضررت جراء شن هجوم عليها، فإن هوية المهاجم ستظل محاطة بالغموض.

وعلى أية حال ليس بمقدور حرب التحكم الآلي أن تقتل وحدها شخصا، أو تدمر أكثر مما ينبغي، ولا يمكنها أن تحتل أراض أو تغير نظاما، بيد أنها قادرة على إتاحة الفرصة لاستخدامات أخرى، وتلك الاستخدامات تكون ملموسة جدا. ومن الجدير بالذكر أن غالبية عمليات التحكم التي وقعت كانت ترمي لسرقة معلومات أو استخدام الحواسيب الهدف، وفي نفس الوقت إبقاء الأجهزة مثلما كانت عليه. وبالإمكان ترتيب هجمات تحكم آلي من أجل تضليل أشخاص – مثل بث صور رادار مزيفة. وفي حالات أخرى قد تعمل هذه المسألة كسيف ذي حدين، فمنذ اللحظة التي يتم التأكيد من أنك نجحت في خداع شبكة ما فإن مديري هذه الشبكة لن يسمحوا لها بالبقاء عاملة مثلما كان الوضع عليه.

هل " دودة" ستاكسنت هي نموذج غير عادي؟

يمكننا القول أن هجوم التحكم الآلي الذي تمكن من تشويش عمل شيء بصورة عملية، اجتاز المرحلة التي يمكن لأية جهة أن تقلل من شأنها. لقد تم اكتشاف دودة ستاكسنت خلال شهر حزيران 2010، وفي أيلول تم اكتشاف هدفها: منشأة نووية إيرانية. وقد أشارت الشبهات الأولية إلى أن مفاعل بوشهر هو الهدف[1]، لكن إيران نفت أن يكون المفاعل قد أصيب بأية دودة. وبعد بضعة أسابيع عرف أن مفاعل أجهزة الطرد المركزية الخاصة بتخصيب اليورانيوم في نتناز هو هدف الهجوم. وقد فند النفي الإيراني في نهاية تشرين الثاني 2010 حينما قام شخصان باغتيال عالم إيراني نووي، وحينما اعترف أحمدي نجاد بأن دودة حاسوب ألحقت أضرارا جسيمة، بيد أن إيران أصلحتها[2]. ترى ما هو حجم الأضرار التي ألحقتها دودة ستاكسنت بالتطوير النووي الإيراني؟ تشير إحصائيات وكالة الطاقة النووية العالمية إلى أن من الجائز أن الدودة المذكورة تسببت في استهلاك مسبق بنسبة 10% من أجهزة الطرد المركزية الإيرانية، الأمر الذي منح صانعي الدودة

[1] Robert McMillan, IDG News, "Was Stuxnet Built to Attack Iran's Nuclear Program? " taken from PCWorls September 21, 2010
[2] William Yong, Alan Cowell, "Bomb Kills Iranian Nuclear Scientists" New York times, November 30, 2010.

بضعة أشهر من التأخير في جدول عمل عملية تخصيب اليورانيوم الإيرانية. وقد أفادت شخصيات رفيعة في تقارير أخرى أن الموعد الذي يمكن لإيران أن تركب فيه قنبلتها النووية هو 2015، أي أن الدودة أحدثت تأخيرا لبضع سنوات.

إن ما هو معروف حول دودة ستاكسنت هو غيض من فيض – باستثناء ما أحدثته من أضرار- فليس من الواضح كيف نجحت الدودة في التسلل إلى مفاعل نتناز. وهناك شبهات تشير إلى أن صانعي الدودة تلقوا مساعدات عن قصد أو عن غير قصد من مقاولين روس، وأنهم تمكنوا من تخريب المفاعل عبر التعاون معهم. والأهم من ذلك هو من هي الجهة التي أشرفت على صناعة هذه الدودة، ومن الذي أطلقها؟ هل هو شخص ما؟ رغم أن مقدرتها وعملها يؤكدان غير ذلك. هل كانوا الإسرائيليين مثلما يمكن التخمين من عدة إلماحات في الرموز الأصلية في الدودة؟ أليس من الجائز أن صانعي الدودة زرعوا تلك الرموز من أجل التضليل؟ هل كانوا الأميركيين؟ وهل من الممكن أن هناك تعاونا أميركيا إسرائيليا على هذا الصعيد؟ إن الغموض الكبير الذي يلف هذه القضية جعل الإيرانيين لا يستطيعون الرد على أي من تلك الأسئلة حتى الآن. ويجب أن نذكر أن سورية لم ترد على الهجوم الذي شن على مفاعلها النووي، وأيضا العراق لم تفعل سوى أن قدمت شكوى للأمم المتحدة في أعقاب قصف مفاعلها النووي "أوسيراك"، هذا رغم أنه لم يكن هناك أي غموض بالنسبة للمنفذين.

إن ميزة استخدام دودة ستاكسنت بدلا من استخدام القوات الجوية لتقليص المقدرة النووية الإيرانية واضحة جدا، وذلك على افتراض أن الدودة فعلت ما أمل صانعوها أن تفعله.أضف إلى ذلك أنها تمكنت من زرع عدم الثقة في أوساط ضحاياها وضبابية حول الجهة التي تعاني من الدودة من بين مزودي المعلومات أو التجهيزات المستخدمة، وكل ذلك يتم بدون أية إمكانية لشجب جهة ما، بل وبنوع معين من التقدير الخفي، وبمخاطرة أقل على الصعيد الاستراتيجي من المخاطرة باستخدام القوات الجوية.

استخدام الغموض:

إن التخمينات تشير إلى أن هجمات التحكم الآلي التي تستخدم بدلا من الأساليب المتحركة المعروفة تخلق غموضا كبيرا جدا على صعيد النتائج والمصادر والأسباب. لذا فإذا عملت هجمات التحكم الآلي بصورة فعالة، فإنها تغير طبيعة الأخطار لعمليات معينة، وبصورة تجعلها بدائل أكثر ملائمة للعمليات. ونورد فيما يلي بعض النماذج النظرية لهجمات تحكم آلي:

أ- يمكن لضحايا هجمات التحكم الآلي أن يستخدموا هجمات التحكم الآلي من أجل الرد والإعراب عن الاستياء دون تحمل أية مخاطر تصعيد أو تحمل مخاطر تصعيد أقل بكثير من تلك التي لو لجأوا فيها لاستخدام الرد المادي. فعلى سبيل المثال في نهاية عام 2010 قصفت قوات كوريا الشمالية جزيرة في كوريا الجنوبية وقتلوا مدنيين وعسكريين. إن الرد على هذا الهجوم في صورة تحكم آلي ترمي لتشويش منشأة صناعية هامة كان بمقدوره أن ينقل استياء كوريا الجنوبية. ولو أن كوريا الشمالية أرادت الرد على هذا الهجوم لتوجب عليها: 1) أن تعترف بأن إحدى منشآتها قد اخترقت.2) أن تتخذ خطوات تؤكد أن كوريا الجنوبية هي المسؤولة الوحيدة عن ذلك، في حين أن من الممكن أن تكون المسؤولة عن ذلك الولايات المتحدة أو الصين أو أية دولة أخرى. وإذا لم ترد كوريا الشمالية بصورة علنية، فسوف يصبح لديها فرصة للحد من عدد الذين يعرفون ما عدد المنشآت التي توقفت عن العمل.

إن هذا الوصف هو بمثابة عامل مميز هام لحرب التحكم الآلي والذي يمنحها أولوية على الحرب المادية، حيث أن تعرضك للهجوم المادي قد يكون مصدر فخر لك، فحقيقة اختراقهم لأجهزتك يعني أنك دخلت إلى مجال التحكم الآلي دون أن تنتبه للدفاع عن منشآتك، وتجهيزاتك. إن الضحايا في حرب التحكم الآلي لا يستحقون أن يفخروا بما حدث لهم، وبناء عليه فإن من الأفضل للدول القادرة على إخفاء تعرضها للهجوم أن تفعل ذلك مما يتيح لها إمكانية الحفاظ على كرامتها. ولا شك أن هذا الطريق يفتح أمام هذه الدول كي ترد بصورة مماثلة.

ب-بمقدور الدول التي يتوفر لـديها محـاربو تحكـم آلي أن تهـدد باسـتخدامهم للـردع إذا حـاول أعـداؤها تحويلها إلى هدف محتمل. فعلى سبيل المثال بمقدور إسرائيـل أن تهـدد إيـران بهجـوم تحكـم آلي إذا هاجمهـا حـزب اللـه الذي يرتبط بإيران بأواصر قوية. ومن الممكن في مثـل هـذه الحـالات أن لا تكـون إسرائيـل معنيـة بـنشر هـذا التهديد على الملأ، فالتهديد العلني يمكنه أن يتيح الفرصة لحزب اللـه لفرض إرادته على طهـران بـدعوى أنـه معنـي بإبراز الضربة التي ستدفع إسرائيل لمهاجمة إيران في مجال مماثل. إن المشكلة في حرب التحكم الآلي تكمن في إمكانية تحديد الجهة التي شنت الهجوم أولا، وذلك على عكس الهجمات المادية المعروفة، كأن يطلـق حـزب اللــه صـواريخ على إسرائيل، حيث يسهل تحديد الجهة التي أطلقتها.

ورغم أن دولة كإيران قد لا تخشى الهجوم الإسرائيلي المباشر حتى لو كان ردا عـلى الهجـوم الـذي سيشـنه حزب اللـه عليها، فقد تبدو خائفة من هجمات تحكم آلي آخذة بعين الاعتبار الكفاءة العالية التي يتمتع بها مخترقو التحكم الآلي الإسرائيليون مقارنة بنظرائهم الإيرانيين. ولا شك أن هذا التفوق بيِّن، ولا يلغي المخاوف مـن أن لا تجـد إسرائيل أهدافا في طهران لمهاجمتها رغم إعلانها عن نيتها الهجوم. ورغم أن نجاح الهجمات المنفردة ليس مؤكـدا، إلا أن هناك فرصة كبيرة لأن يتمكن قسم من الهجمات من تحقيق نجاح وإلحاق أضرار جسيمة.

إن توجيه إيران أصابع الاتهام للولايات المتحدة يمكنه أن يخلق مشكلة للولايات المتحدة وفي نفس الوقت يسهل الوضع على إسرائيل. ولا شك أن تصعيد أعمال العنف بالنسبة لإيـران ليسـت خيـارا نظـرا لأنهـا تعـرف مـدى التفوق الإسرائيلي في مجال الحرب التقليدية. ومن ثم ستضطر إيران للاعتراف بأن تجهيزاتها خربت وأن تقنع الجميع بأنها تعرف من هي الجهة التي تقف خلف هذه العملية. ونظـرا لأن شـبكات إسرائيـل الداخليـة للحواسـيب أوسـع بكثير من إيران، إلا أن هذا لن يمنح إيران تفوقا إذا حاولت شن الهجوم.

ت- بمقــدور هجــوم الــتحكم الآلي أن يخــدم إحــدى الــدول كي تــؤثر عــلى نتــائج نــزاع داخــل دولــة أخرى دون أن تضطر للالتزام بذلك علنا. فعلى سـبيل المثـال الحـرب في ليبيـا، فلـو أن الجـيش الليبـي كـان مربوطـا

للانترنت بصورة تجعل هجمات التحكم الآلي قادرة على التأثير على أدائه، لأصبح بالإمكان شن هجوم تحكم آلي يعجز قوات الحكومة المركزية وإمالة الكفة لصالح القوات المعارضة له. ولو أن المتمردين انتصروا في هذه الحالة لكانت الدول الغربية هي صاحبة الفضل في ذلك. ومن الجائز أن قوات المتمردين ما كانت لتعرف أنها تلقت مساعدة. وهناك إمكانية أخرى لإرسال رموز، كأن يقال للمتمردين: إذا ما تم شل هذه الجبهة أو تلك، فيجب أن تعرفوا أن السبب في ذلك هو نحن.

ولو أن قوات النظام هي التي انتصرت، فكانت ستشك بأن قوات الغرب قامت بتخريب منظومات معلوماتها، لكنها لن تكون قادرة على إثبات ذلك. وكان من المتوقع أن تقوم ليبيا بتوجيه أصابع الاتهام للغرب، بيد أن عدم تمكنها من تقديم الدليل على شكواها، لن تولي أية جهة اهتماما للشكوى.

مجال التحكم الآلي والمنظمات الإرهابية

تحكي قصة الفيلم المسمى "أموت لأحيا مرتين" الذي عرض في الولايات المتحدة عام 1990 حكاية إرهابيين يسيطرون على منظومة حاسوب، رقابة المواصلات، والاتصالات الجوية، ويدعون أنهم مراقبو طيران، ويعطون الأوامر الكاذبة، ويوجهون الطائرات للتحطم على المدارج بركابها وسط عاصفة ثلجية. لقد وقفت قوات الأمن عاجزة عن تقديم أية مساعدات، بما فيها بطل الفيلم، الذي لم يكن أمامه في نهاية المطاف سوى الوقوف عاجزا على المدرج ممسكا بمشعلين بيديه ملوحا بهما للطائرة المقتربة من الكارثة.

قد يقول قائل أن هذا الفيلم هو مجرد فيلم مبالغ فيه، بيد أن أحداث الحادي عشر من أيلول 2001 والتغييرات والتطورات التي طرأت على التهديدات الأمنية خلال العقد الماضي تؤكد أن الأفلام الأكثر خيالية في السينما يمكنها أن تجد طريقها على أرض الواقع في أيامنا هذه.

إن استخدام حرب التحكم الآلي بين الدول المتخاصمة أو المتعدية كساحة حرب مركزية كان دائما وأبدا يعتبر بمثابة أرض خصبة لأفلام الخيال العلمي. لكن هذا المجال الذي كان فخر صناعة الأفلام في هوليوود بدأ يحتل مكانا مركزيا في إحدى الساحات الهامة التي ستدور فيها – على ما يبدو- حروب المستقبل بين

الجهات المختلفة والتي من بينها المنظمات الإرهابية، التي لجأت حتى الآن في عملياتها للجانب المادي العنيف من أجل تحقيق مصالحها.

وإزاء هذه التهديدات، عمدت الدول الغربية إلى إقامة خلال السنوات القليلة الماضية هيئات خاصة يجب عليها أن تعد العدة لمواجهة أعمال حربية تستخدم فيها المعدات التكنولوجية الجديدة ضد أهداف مادية إستراتيجية. وسوف نناقش في هذا البحث إمكانية أن تقوم المنظمات الإرهابية باستخدام مجال التحكم الآلي لمهاجمة بنى حساسة في دول، ومؤسسات ورموز سلطة، ومنظومات عمل وصناعة، وأهداف مدنية عامة مختلفة.

تهديدات التحكم الآلي من قبل المجموعات الإرهابية:

هناك خمس مجموعات تستخدم حاليا أو أنها ستستخدم في المستقبل وسائل حرب التحكم الآلي، وهي: 1-الدول التي تطور مقدرة هجومية ودفاعية كجزء متنامي في أطار تفعيل قواتها. 2- جهات جنائية تحركها مصالحها النائية والعملية بصورة أساسية 3- شركات الأعمال العاملة بصورة رئيسة في مجالات الدفاع نظرا لأن هجمات التحكم الآلي في مجال قطاع الأعمال في حالة زيادة مضطردة، وقسم منها يتجه نحو مهاجمة الشركات المنافسة 4- المنظمات الإرهابية والتي يمكنها أن تحاول تنفيذ هجمات إرهابية عبر التحكم الآلي نظرا للقوة والجدوى لاستخدام هذا النوع من الأسلحة بالنسبة لها. 5- الجهات الفوضوية التي تعارض الأجهزة المؤسساتية القائمة، وهي معنية بتخريبها من الداخل أو من الخارج، وستعمل على مهاجمة منظومات حواسيبها التي تعتبر حاليا بمثابة قاعدة الإدارة بغية تشويش وتدمير النظام الاجتماعي والخيوط التي تربط بين حياة المواطنين في الدولة.

إن مجال حرب التحكم الآلي الذي من المحتمل أن تدخل إليه المنظمات الإرهابية يحمل في أحشائه احتمالات التغيير في موازين القوى في المجتمع، نظرا للقوة التي يمنحها للمهاجمين، وبشكل خاص للمنظمات الإرهابية التي تعمل مستخدمة قوة أقل كثيرا من القوى التي تحاربها، وبعدم تناسب على هذا الصعيد بين الجانبين.

إن بناء مقدرة في هـذا المجـال يمكنـه أن يتـيح الفرصـة للمـنظمات الإرهابيـة لمهاجمـة منشـآت، ومواقـع خصومها وإلحاق أضرار مادية شديدة بها وخلق تأثير نفسي هائل على المجتمع الذي يتعرض للهجوم، وكل ذلك يمكن أن تفعله إضافة إلى استخدام الوسائل المعروفة لنا حاليا والتي تستخدمها في إطار الحرب التقليديـة، مثـل العمليـات الانتحارية، وتفعيل العبوات الناسفة، احتجاز الرهائن، عمليات الاختطاف لوسائل المواصلات والأشخاص.

هناك العديد من المزايا لهجمات التحكم الآلي:

أولا: تجنب التواجد المادي في مكان الهدف الذي تقوم بمهاجمته، حيث أن بالإمكان القيـام بـالهجوم عـن بعد بشبكات الاتصالات وأجهزة الرقابة الخاصة بالمنشـآت، ومـن ثـم الامتنـاع عـن ضرورة مواجهـة العوائـق الماديـة والمعارك البشرية.

ثانيا: حجم الأضرار، هجوم التحكم الآلي لا يقع فقط في فضاء مادي بل أيضا لديه الإمكانية لإلحـاق أضرار شديدة ومتواصلة بمنظومات الرقابة والبنى التحتية. وفي الوقت الذي تحدد فيه العمليـات الإرهابيـة بزمـان ومكـان، فإن هجوم التحكم الآلي يعزز جانب الرعب والترهيب المرتبطين بالتأثيرات النفسية للعمليات الإرهابية.

ثالثا: إخفاء مصدر وهوية الجهة المهاجمة. ففي مجال الـتحكم الآلي مـن الأسـهل تمويـه وإخفـاء الحـدود والهوية القائمة بين الدول، فبمقدور الجهات الإرهابية أن تشن هجوم تحكم آلي في الوقت الـذي تخفـي فيـه هويتهـا والقيام بعمليات تمويه تتعلق بمصدر الهجوم، مثل القيام بهجوم في الدولة الهدف مع استخدام عناوين دولة صـديقة مما يصعب على الجهة التي تتعرض للهجوم تشخيص المصدر الحقيقي للهجوم.

رابعا: علاقة تفوق وجدوى على أفضل الصور مـن قبـل المـنظمات الإرهابيـة المتدنيـة في قوتهـا ومواردهـا مقارنة بالجهات التي تهاجمها إذا تمكنت من استخدام التحكم الآلي من أجل مهاجمتها. وعـلى افـتراض أن المـنظمات الإرهابيـة ستفضـل اختيـار الأهـداف الأقـل حمايـة فـإن بمقـدورهم شـن الهجـوم بعـد خلـق إمكانيـة وصـول إلى

الهدف، وإدخال أشخاص كي يزرعوا "رموزا شريرة" للعمل في المواقع الهدف، أو استخدام التكنولوجيا التي يمكن القول أنها متوفرة لقطاعات جماهيرية واسعة.

خامسا: إرهاب دون قتل، حيث بمقدور المنظمات الإرهابية شن هجوم تحكم آلي تلحق به أضرارا جسيمة دون أن تمس ماديا وتقتل بصورة مباشرة. وبذلك بمقدوره تحقيق إنجازات عبر الترهيب وتشويش طبيعة الحياة مما سيمنح المنفذين مقدرة دفاعية وتبريرا لأعمالهم دون أن يسفكوا نقطة دم واحدة. ولا شك أن العملية ستوفر دعاية كبيرة وواسعة للمنظمة الإرهابية، وإدخالها في إطار عمليات المساومة.

هناك من يقول أن المنظمات الإرهابية غير معنية بمجال التحكم الآلي نظرا لأنها تفضل العمليات الاستعراضية لسفك الدماء، والتي تثير الرعب أكثر بكثير من العمليات الخفية التي تخوضها هذه الجهة أو تلك عبر التحكم الآلي، بيد أن هذا الزعم لا يتساوق مع النظرية الأساسية لاستخدام إستراتيجية الإرهاب، والتي تنص على أنه يتوجب على العمليات الإرهابية التركيز على محاولات تقليص فوارق القوة في النضال ضد خصم يتمتع بقوة أكبر، عبر القيام بعلميات أكثر تدميرا مع البحث عن نقاط الضعف في جهازه الدفاعي من أجل التسلل عبرها والتمتع بموقف تفوق بثمن يمكن تحمله ويتناسب مع الوسائل القليلة نسبيا التي تملكها الجهات الإرهابية.

ويمكننا أن نرى اليوم أن منظمات من الجهاد العالمي تقوم باستخدام واسع النطاق – وإن لم يكن متطورا إلى حد كبير- بمجال حرب التحكم الآلي من أجل تحقيق المزايا الكامنة به. لقد أشار البحث الذي تفحص القدرة والاستخدام لمجال التحكم الآلي في منظمات الجهاد[3] إلى وجود مميزات أساسية تستخدم لبناء وتحسين البنى التنظيمية التنفيذية للمنظمات الإرهابية في المجالات التالية:

- الدعاية: استخدام من أجل نشر أفكار، قرارات، توجيهات، خطابات وآراء رجال الدين وزعماء الإرهاب.

[3] Examining the Cyber Capabilities of Islamic Terrorist Groups, Institute for Security Technology Studies at Dartmouth College March 2004

- التجنيد والتدريب: استخدام بغية العثور على أعضاء محتملين وتجنيدهم، ونقل مواد تأهيل وتدريب بواسطة الشبكة.
- جمع الأموال والتمويل: استخدام الشبكات بغية جمع المبالغ المالية تحت غطاء منظمات صدقة ومعونة مع استخدام بطاقات ائتمان.
- الاتصالات: استخدام الشبكة كجهاز اتصال تنفيذي مع استخدام تجهيزات متنوعة ومن ضمنها أجهزة تشفير متوفرة.
- العثور على أهداف ومعلومات استخبارية: استخدام المعلومات في الشبكة من أجل العثور على أهداف وإجراء أبحاث استخبارية.

إن انتقال المنظمات الإرهابية من الاستخدام اللوجستي والدعائي للاستخدام العملي بواسطة معدات تحكم آلي يمكنه أن يتجسد في صورة عمليات درامية جديدة ورخيصة الثمن، وفي نفس الوقت تحظى بتعاطف كبير ومن الجائز أن تلحق أضرارا أكبر. لذا فإن كل منظمة إرهابية - وبشكل خاص تلك التي تتطلع إلى الدعاية وخلق تأثير نفسي على جماهير خصومها ترى في مثل هذه العملية بمثابة تحد هام وتطلع يستحق الاهتمام ويجب بذل الجهد من أجل الوصول إليه وتحقيقه. والتجديد سيضمن أيضا للمنفذين انتشارا وإعلاما دويا بوصفهم نموذجا يجب الاقتداء به. وبناء على ذلك فإن المنظمات السياسية التي تعتبر مقدرتها التكنولوجيا أقل من الدول التي تخوض حروبا ضدها ، قد تعمد إلى الانضمام إلى اتجاهات تستغل التكنولوجية الحديثة المطلوبة لحرب التحكم الآلي لكن ليس كشرط ضروري، وذلك من أجل الاستعانة بدول متقدمة أو شراء أشخاص وجهات ذات مقدرة على إبراز البراعة والتفوق في هذا المجال.

والدول الداعمة للإرهاب تشعر بانجذاب كبير جد أيضا إلى مجال التحكم الآلي، فالغموض الذي يلف استخدام حرب التحكم الآلي، وصعوبة إثبات الجريمة على الفاعل، وإمكانية النفي العالي التي تتمتع بها

الدول على هذا الصعيد لتورطها، وإمكانية إلحاق أضرار جسيمة بالخصم، كل ذلك يبدو عامل جذب إلى هذا الجانب من الحرب. وحتى إذا ثارت شكوك تجاهها فسوف يكون من الصعب إثباته، وفي جميع الحالات فإن عمليات التحكم الآلي تثير غضب الجماهير أقل بكثير مما تثيره العمليات التقليدية الإرهابية بالأسلحة والتي تلحق أضرارا جسيمة وتسفك الدماء، حتى لو كانت الأضرار المادية التي تلحقها عمليات التحكم الآلي أكبر بكثير.

ورغم مزايا هجوم حرب التحكم الآلي التي تطرقنا إليها أعلاه، إلا أننا لم نعلم بأن مخربين قاموا حتى الآن بمثل هذه العمليات. إن بناء مقدرة حقيقية في مجال هجوم التحكم الآلي يتطلب التوصل إلى مقدرة استخبارية وتكنولوجية لا يستهان بها. وفي هذه المرحلة يمكننا الافتراض أن المنظمات الإرهابية تواجه صعوبة في العثور على مقدرة تكنولوجية عالية جدا يسهل التوصل إليها وتنفيذ أهدافها عبرها. حقا أن الاعتماد على مقدرة الدول المؤيدة للإرهاب يمكنه أن يوفر لها مطلبها ولو بصور جزئية، لكنها لا تتيح للمنظمات الإرهابية حتى الآن مخزنا تكنولوجيا كبيرا يمكنها الاغتراف منه بصورة دائمة ومن ثم القيام بعمليات متتابعة وفعالة.

كما تواجه المنظمات الإرهابية قيودا بالنسبة للعمل في مجال حرب التحكم الآلي العلني - عبر الانترنت، ولا شك أن هذا الجانب يعتبر بمثابة نقيصة واضحة وتحد كبير لها، نظرا لأن مقدرة المتابعة والمراقبة الإستخبارية للتحكم الآلي لدى الدول المتقدمة تكنولوجيا تمكنها من ملاحظة وتشخيص المسلكيات المشبوهة على الانترنت، واكتشاف التنظيمات والعمل على حماية نفسها منها ومن تهديداتها.

نقاط ضعف وعلاج:

رغم أن المنظمات الإرهابية لم تنجح حتى الآن في التغلب على العوائق القائمة أمام الحصول على مقدرة هجومية عبر التحكم الآلي، فإن الأهداف المدنية والتي يسهل توجيه الضربات اليها في الحياة تبقى بمثابة أهداف مفضلة لتلك المنظمات. ولا شك أن هذه الأهداف هي نقطة الضعف الأساسية، والقدرة على حمايتها تبقى أقل من حماية الأهداف الأمنية. ويمكننا القول أن تعزيز الحماية على البنى الوطنية الحيوية مثل محطات

الطاقة الكهربائية، والمياه والاتصالات سوف تدفع بالمنظمات الإرهابية للقيام بمحاولات من أجل توجيه ضرباتها إلى أهداف أقل حماية في قطاعات العمل والقطاعات المدنية. ورغم أن في الكثير من الحالات فإن أهدافا من هذه القطاعات غير مشمولة ضمن مؤسسات البنية الحساسة المحمية في الدولة، فإن قيام المنظمات الإرهابية بعمليات ناجحة ضدها يخلق نتائج فعالة وبشكل خاص على صعيد المساس بأمن السكان واحتياجاتهم.

قسم كبير من عملية بناء جهاز الحماية ضد هجمات التحكم الآلي هو بناء عام، ولا علاقة له بمصادر التهديد، سواء كان مصدره المنظمات الإرهابية أو جهات سياسية أو جنائية. وهذا الوضع ينطبق على الجانب التنظيمي كالذي تقوم به سلطة حماية المعلومات والوزارات المتخصصة بالحماية من التحكم الآلي في العديد من الدول، وكذلك الأمر في قسم من آليات الدفاع والحماية في أجهزة المعلومات والحماية العامة. وفيما يتعلق بالمنظمات الإرهابية الراغبة بالقيام بعمليات تحكم آلي، فإنها تحتاج إلى عاملين معينين يتطلبان عملية تطوير وتحسين متواصلة:

مقدرة استخبارية:

إن الحاجة إلى جمع معلومات استخبارية دقيقة ونوعية يتطلب القيام بعمليات جمع متنوعة من مصادر عديدة، ومن ضمنها المصادر العلنية، والمحوسبة ومن شبكات المنظمات الإرهابية. وفي إطار ذلك يجب العمل على تطوير مقدرة للبقاء في هذه الشبكات بصورة خفية وسرقة المعلومات باستمرار وفعالية. ومن أجل ذلك يجب التغلب على الانتشار الواسع والعالمي الذي يميز المنظمات الإرهابية التي تستخدم الكثير من النوافذ في شبكة الانترنت، وتنقل الرسائل المشفرة ذات الرموز الخاصة.

ويجب على الجهات الاستخبارية أن تبني مقدرة اعتراض للرسائل والبث وحل شيفراتها بصورة دائمة وسريعة، وتزويد جهات الحماية من حرب التحكم الآلي بالوسائل التي تمكنها من حماية نفسها من النشاطات والعمليات التي يجري التخطيط لها وتشويشها.

أجهزة التشويش:

إن شبكات الحماية التـي نقيمهـا لا تحـاول منـع هجـمات الـتحكم الآلي بـل تحـاول منعهـا مـن تحقيـق أهدافها، فإن هدف أجهزة التشويش هو إحباط تنفيذ الهجوم أو توجيه ضربات لمساراته.إن إقامـة أجهـزة تشـويش فعالة ضد هجمات التحكم الآلي التي تقوم بها المنظمات الإرهابيـة يتطلـب رقابـة اسـتخبارية قـادرة عـلى تشـخيص وتحديد الهجوم قبل وقوعه، والعمل بفعالية من أجل إحباطه. ويعتمد هذا الجانب بصورة رئيسية على مقدرة جمع المعلومات الاستخبارية التكتيكي سواء كان ذلك في الحواسيب أو شبكات الاتصالات التي تستخدمها شبكات الإرهاب.

تجري عمليات تشويش في الكثير من الحالات غير موجهة إلى محاولات هجوم معينة، بل كمحاولـة لضرب البنى التنظيمية للمنظمات الهدف المعادية، وقد وقعت مثل هذه العمليـات عـلى سـبيل المثـال في بريطانيـا عنـدما قامت المخابرات البريطانية بتخريب صورة غلاف مجلة القاعدة "**Inspire**". وقد تعرضت مراكز الجهاد الالكترونية في الآونة الأخيرة ومؤسساته لهجمات تحكم آلي غالبيتها منسوبة إلى دول غربية:فقـد تـم تخريـب موقـع حركـة طالبـان بصورة متواصلة، كما تعرضت جهات جهادية ومواقع أصولية إسلامية لهجمات تحكم آلي. ومن الناحية الأخرى تقـوم شبكات أميركية وسعودية وهولندية باستخلاص معلومات استخبارية قيمة جدا حول الإرهاب الإسلامي المحتمل مـن مواقع جهادية والتي تستخدم "كمصيدة عسل" - **Honeytraps** للمعلومات الاستخبارية النوعية[4].

ولا شـك أن مـن الواجـب العمـل عـلى تعميـق الحمايـة للمـنظمات المدنيـة والتـي تعتـبر بمثابـة أكـبر نقطة ضعف، مما يجعلها الأهداف المفضلة على المنظمات الإرهابية. فالحكومة البريطانية على سـبيل المثـال شرعـت باتخاذ وسـائل تشريعيـة متعـددة تشـمل المصـادقة عـلى اسـتخدام أجهـزة اخـتراق، مثـل: التنصـت عـلى المحادثـات

---

[4] Adam Rawnsley, "Stop the presses, Spooks hacked al-Qaida online mag" Wired, June 3, 2011

الهاتفية، متابعة البريد الألكتروني في ملفات الشرطة ذات العلاقة بجرائم الإرهاب، تخريب النشاطات الراديكالية على شبكات الانترنت، وتدريب وحدات شرطة خاصة لمواجهة تهديدات حرب التحكم الآلي[5].

ورغم ذلك فإن عمليات الدفاع في غالبية الدول على المنشآت والمؤسسات المدنية، لا زالت في بداياتها، وغالبية موارد الدولة في مجال الحماية من هجمات التحكم الآلي مخصصة للمؤسسات الأمنية وللجهات التي يطلق عليها اسم البنى الوطنية الحساسة. إن تعميق الحماية على المؤسسات المدنية يتطلب استعدادا كبيرا في المؤسسات الوطنية، على أن يتم دعم ذلك بأنماط عمل ملائمة[6].

جرائم التحكم الآلي كتهديد للأمن الوطني

اقتحم مجال التحكم الآلي الذي ولد من رحم تطور تكنولوجيا الحاسوب ووسائل الاتصالات الرقمية حياتنا خلال العقود القليلة الماضية. ووسائل الاتصالات والحوسبة ترمي لتحسين وتفعيل أدائنا بصورة أفضل وهي تدخل في جميع مجالات الحياة وتؤثر على أنماط العمل في جميع المناحي. إن شبكة الانترنت التي تحولت إلى شبكة تجارية عام 1988 ثم نمت حتى أصبحت جزءا هاما في مجال التحكم الآلي تتيح لها إمكانية الوصول الفورية والرخيصة للمعلومات بكافة أنواعها، والمشاركة في المعلومات والعمل المشترك عن بعد وغيره.

ترجع جرائم التحكم الآلي التي يمكن اعتبارها مساسا بالأمن القومي إلى قيام جهات ذات توجهات معادية لاستخدام هذا المجال من أجل إلحاق الأضرار. وسوف نتطرق في هذه الدراسة إلى التعاون بين المجرمين والجريمة المنظمة والمنظمات المعادية، والمتاجرة بإمكانية الاعتداء عبر التحكم الآلي الذي يصبح ممكنا جراء التطور التكنولوجي ونمو "السوق الأسود" لخدمات الحاسوب. والحقيقة هي أن جرائم حرب التحكم الآلي لا تشكل خطرا على الأمن الوطني حاليا، بيد أن هناك شرطين إذا توفرا ستتحول جرائم حرب التحكم الآلي إلى تهديد للأمن الوطني.

---

[5] "Warning of rise in cyber-terrorism" The independent, July 12, 2011

[6] جابي سبوني: "حامية الممتلكات والبنى الحساسة من هجمات التحكم الآلي" الجانب الإداري، مركز أبحاث الأمن القومي المجلد -3 العدد1 آيار 2011

تزداد مطالب وحاجة الجماهير إلى الأمن في مجال التحكم الآلي كلما ازدادت معرفتها للتهديدات القائمة، وحتى لو لم نشهد ارتفاعا في جرائم التحكم الآلي، فلا يمكننا أن نفترض أن هذه المطالب ستتضاءل. إن مسؤولية الدولة تجاه مواطنيها لا تتوقف في مجال التحكم الآلي. وحتى في هذا المجال يجب تحديد انعكاساتها العملية وفقا لمسار سياسي ديمقراطي يقوم على أسس واقعية قوية.

ظاهرة جرائم التحكم الآلي:

لم تتجاوز التكنولوجيا المحوسبة التي وضعت من أجل تغيير وتحسين مسارات الإنتاج والعمل في جميع مناحي الحياة عن عالم الجريمة. إن الحوسبة تتيح فرصة تفكيك المهام إلى جزيئات صغيرة وتفصيلات دقيقة، والشبكات تسمح بوصول عالمي إلى المعلومة والتركيز عليها بوصفها منتجا ذا قيمة. والتحديد المقترح لجريمة التحكم الآلي هي: استخدام مجال التحكم الآلي لأهداف محظورة، مع استغلال البرامج الخاصة التي تميز مجال التحكم الآلي القائم مثل: السرعة والفورية، التفعيل عن بعد، الشيفرة والإخفاء التي تسهم في خلق صعوبات في تشخيص أعمال المستخدم، استغلال القيمة المتصاعدة للمعلومات الرقمية على أنواعها، المعالجة القانونية والقضائية المختلفة في مجال التحكم الآلي في الدول المختلفة.

هذا ولا زالت عملية تحديد ووصف ظاهرة جريمة التحكم الآلي تواصل تطورها. لقد تساءل جربوسكي قبل أكثر من عقد حول ما يمكنه أن يستجد في مجال جرائم التحكم الآلي، وقال:أليست هذه الظواهر هي ظواهر قديمة تستخدم تجهيزات جديدة؟[7] بيد أن غالبية الباحثين يحاولون تحليل جريمة التحكم الآلي بوصفها ظاهرة خاصة. وقد قام ماجي ديار بتصنيف الجريمة وفقا للشيء المصاب: ضد الممتلكات، ضد بني البشر، ضد الدولة[8] . أما شيندر وكروس فصنفا الجريمة وفقا لمستوى العنف: عنيف، عنيف ومحتمل، غير محتمل –

---

[7] P.N. Grabosky, Virtual Criminality: Old Wine in New Bottles? Social and Legal Studies, 10\2\2001

[8] Majid Yar, Cybercrime and society: crime and Punishment in the information age London: Sage Publications 2006

تجارة مخدرات، غسيل أموال- سرقات اقتحام وغش-[9] . لقد تطورت جرائم التحكم الآلي في أعقاب نمو وسائل الاتصال والحاسوب ومجال التحكم الآلي، والإمكانيات الجديدة للحصول على المعلومات، أو التشويش واحتكار المعلومات لأغراض الربح. وقد قام وول بتصنيف جريمة التحكم الآلي في ثلاثة نماذج:جرائم تتعلق بسلامة وفعالية منظومات الحاسوب - Hacking اقتحام المنظومات- جرائم تستعين بمجال التحكم الآلي – وسائل اتصالات مشفرة بين مجرمين، بيع علاجات مزورة، جرائم تتعلق بمحتوى المعلومات المحوسبة – سرقة أسرار، نشر برامج ضارة.

ويمكننا أيضا أن نصنف الجرائم وفقا لوظيفة الحاسوب، وقد تبن الميثاق الأوروبي ضد جرائم التحكم الآلي توجها مشابها[10]:

الحاسوب كوسيلة لتنفيذ جرائم:

التوجه إلى، ونشر محتوى	تشويش المعلومات أو المنظومات	استخدام وسائل الإعلام
أسرار	عن قصد وسبق إصرار	مضايقات
معلومات	انتحال شخصيات	المتاجرة بمواد ممنوعة
معرفة	غش	بريد الكتروني غير مرغوب فيه

الحاسوب كهدف لتنفيذ جرائم:

وصول غير مسموح به	إدخال رمز شرير عمدا	تشويش عمليات	سرقة خدمات:

[9] M.Cross, D.L. Shinder, Scene of the cybercrime. Burlington, MA: Syngress, 2008
[10] Offences against the confidentiality, integrity and availability of computer data and systems

Hacking	تجسس، أضرار، فيروس	DDoS	استخدام غير مسموح به

ومن الجدير بالذكر أن قسما كبيرا من جرائم التحكم الآلي لا تشكل ظاهرة خاصة أو جديدة: المضايقات، الغش، الدعاية المحظورة، أفلام الجنس، السرقات، غسيل الأموال، التجسس وغيره. وكل هذه الأعمال تستخدم مجال التحكم الآلي. أما العامل الإضافي فهي ظواهر لم يكن بالإمكان تنفيذها دون مجال التحكم الآلي: البريد غير المرغوب به Click fraud، برامج شريرة Malware بأنواعها، شبكات حاسوب "مأسورة" Botnet[11]، انتحال شخصيات رقمية، تمويه وتشفير معلومات ووسائل إعلام، اقتحام محوسب لمنشآت محمية ذات قيمة كبيرة والتجسس الأوتوماتيكي المتواصل في المنظمات المحمية والذي يعمل على إخراج ممتلكات ثقافية من سيطرتهم.

إن جرائم التحكم الآلي بجميع أنواعها هي ظاهرة اجتماعية شائعة. وتفسيرات علم الجرائم يرفق بها حوافز، وفرص سانحة ووجود حارس. ويمكننا أن نشخص مصدرين للحوافز الإنسانية للعمل. ويمكننا القول أن قسما كبيرا من محفزات العمل بصورة إجرامية ترجع إلى عوامل شخصية داخلية (Intrinsic Motivation) ولا يتم تحديدها من خلال عملية تمحيص ودراسة للجدوى. فلا يوجد أي سبب يجعلنا نفترض أنه وفي أعقاب الاستخدام المكثف لهذا النوع من التكنولوجيا أو ذاك فإن طبيعة الإنسان ستتغير، لذا ليس من المفاجئ أن يستخدم بني البشر مجال التحكم الآلي لسد احتياجاتهم والسعي وراء أهدافهم سواء كان ذلك في المجالات النمطية، مثل التعليم، التسلية، الثقافة والعمل، أو في الأعمال القديمة التي يمارسها بني البشر مثل القتال والجريمة.

[11] يتعلق الأمر بعدة حواسيب مصابة ببرنامج حاسوب "شرير" يتيح الفرصة للمقتحم للسيطرة عن بعد عليها واستخدامها لأغراضه.

وتقوم المدرسة الكلاسيكية في علم الجريمة على فكرة الاختيار الحر والتقدير المنطقي للجدوى المرتقبة مع فرص العقاب، وتفسر الحوافز التي تحث على تنفيذ الجرائم بوصفها قرارا اقتصاديا منطقيا[12]. ويعكف الاقتصاديون والمحللون النفسيون على تحليل مسلكيات البشر بما فيها الأعمال الإجرامية المستقاة من تقديرات الجدوى المنطقية. ولا شك أن مجموعة الظروف الخارجية المتغيرة يمكنها أن تشجع الجرائم المرتكبة عبر التحكم الآلي: وهذا يحدث حينما يلاحظ الإنسان أن هناك احتمالا كبيرا للربح، ويعتقد أن الثمن وفرصة العقاب أقل في قيمتهما من الجدوى التي سيجنيها. إن توسيع مجال المعرفة الرقمية، وارتفاع قيمة المعلومات المحوسبة يخلقان وضعا يجعل الحوافز الخارجية للقيام بأعمال إجرامية ترتفع.

ورغم أن هناك أجهزة لفرض القوانين في الدول المتقدمة في مجال التحكم الآلي إلا أن رد الدولة لم يجار بعد التغييرات التكنولوجية. وأفضل النماذج لذلك هو المقارنة بين عملية سرقة بنك تقليدية مقارنة بسرقة عبر التحكم الآلي. فسرقة المال من أحد أفرع البنوك ترتبط بإمكانية التغلب على وسائل الحماية، وهي تحمل احتمالا كبيرا لإمكانية الدخول في مواجهة مع الحراس المسلحين، وحتى لو انتهت عملية السطو بنجاح، فإن اللصوص سيتعرضون لسنوات طويلة لعملية الملاحقة من قبل سلطات القانون. لقد أدى تطور مجال التحكم الآلي إلى إتاحة الفرصة لسرقة البنوك والمؤسسات المالية أيضا عبره، فعلى سبيل المثال بات شائعا استخدام شبكات "الحاسوب المأسورة **Botnet** لعمليات سرقة متواصلة لعلامات وأرقام سرية في المواقع البنكية، واستخدامها لسرقة مبالغ مالية صغيرة. وإزاء مشكلة "التأكد من الهوية" – **Attribution** - في مجال التحكم الآلي، وإمكانية اكتشاف المجرم باتت ضئيلة جدا[13]. ومن الجدير بالذكر أن المؤسسات المالية على اطلاع على المخاطر المذكورة، وهي تتخذ الخطوات الاحتياطية اللازمة للدفاع عن نفسها، وتنفق مبالغ كبيرة على حماية المعلومات

---

[12] Piquero, Alexis Russell, and Stephen G. tibbetts. Rational Choice and Criminal Behavior: Recernt Research and Future Challenges. New York: Routledge 2002

[13] Davis S. Wall, Cybercrimes: The transformation of crime in the information age, p. 221

من أجل تقليص مجال وفرص السرقة عبر التحكم الآلي. ورغم ذلك فإن المخاطرة المادية الذاتية الفورية التي يتحملها لصوص التحكم الآلي أقل بكثير من تلك التي يتحملها اللصوص العاديون.

حجم جرائم التحكم الآلي والأضرار-تقديرات مثيرة للجدل:

يتم فحص جرائم التحكم الآلي بصورة عامة من منظور قضائي – تشريع وعقاب- ،علم الجريمة – الأسباب والتنظيم، اقتصادي – محفزات وقيمة- أو تقني – حماية المعلومات. ويعكف القضائيون على وضع حدود للمسلكية المقبولة والقضايا القانونية الخاصة بالمنع وفرض القانون. وعلم الجريمة يطبق المعلومات المهنية لفهم الظواهر الجديدة. أما الاقتصاديون فيصفون العوامل المحفزة والمؤثرة على مسارات اتخاذ القرارات للأشخاص. ويعمل رجال حماية المعلومات على قضايا تقنية للبنى التكنولوجية: البرامج، المواد والاتصالات، مع التركيز على احتمالات الأضرار التي قد تلحق بهذا الجانب أو ذاك، ووسائل الحماية. ويتفق القضائيون، الاقتصاديون ورجال حماية المعلومات في الرأي على أن حجم جرائم التحكم الآلي وشدة الأضرار التي يلحقها في حالة تصاعد سريعة مستمرة.

وتستند التقديرات على حقيقة أن حجم المعلومات الرقمية ازداد بوتيرة كبيرة جدا، وكذلك ربط الأنظمة المحوسبة يتنامى. ويتضمن مجال التحكم الآلي الكثير جدا من المعلومات كما يتضمن الكثير من نقاط الوصول المحتملة للاختراق غير المسموح به. والنتيجة هي أن كل اختراق يكشف المزيد من المعلومات. ومن الجدير بالذكر أن التقديرات المالية لحجم أضرار جرائم التحكم الآلي تنشر منذ سنوات التسعينات وحتى اليوم. وتقوم شركات الأبحاث بإجراء العديد من الأبحاث في هذه القضية، وتنشر تقارير واسعة جدا. وهناك عشرة تقديرات مختلفة مصدرها في القطاعات التشغيلية والحكومية في الولايات المتحدة وبريطانيا ودول متطورة أخرى[14]. وتفيد تقديرات بحث المباحث الفدرالية أن حجم الأضرار التي لحقت بالأعمال الأميركية بلغ 65 مليار دولار عام 2005[15].

[14] انظر على سبيل المثال تقرير GAO, 705-07 – Cybercrime الصفحة 16-17 حزيران 2007.

[15] 2005 FBI computer Crime Survey, p.10

ويقول وزير التجارة الأميركي جاري لوك أن الأضرار السنوية التي تصيب الشركات الأميركية جراء عمليات التزوير وأعمال القرصنة – الاستخدام غير المشروع لرموز الحاسوب- يتراوح بين 200-250 مليار دولار.

وتشير التقارير البريطانية إلى أن حجم الأضرار التي لحقت بالشركات البريطانية بلغ 27 مليار جنيه إسترليني سنويا. أما الأضرار السنوية التي لحقت بالمواطنين البريطانيين فبلغت 3.1 مليار جنيه إسترليني، وقطاع الأعمال 21 مليار جنيه إسترليني، والحكومة البريطانية 2.2 مليار جنيه إسترليني. وقد قدرت الأضرار المالية المباشرة التي تسببها جرائم التحكم الآلي في التقرير الذي أصدرته شركة سيمنتك – التي تعتبر بمثابة شركة رائدة في سوق حماية المعلومات – بمبلغ 114 مليار دولار سنويا في 24 دولة. وهناك تقديرات أخرى تفيد أن حجم المبالغ تصل إلى مئات مليارات الدولارات.

لقد أثارت هذه المبالغ الهائلة الكثير من التساؤلات والشكوك، لكن تأثير الانتقادات حتى الآن لا زال محدودا. وقد نشرت في الآونة الأخيرة ورقة عمل صادرة عن باحثين من شركة ميكروسوفت والتي قامت بتحليل البنية الهشة القائمة على تقدير أضرار جرائم التحكم الآلي عبر الاستطلاعات والأبحاث. ترى كيف يتم حساب هذه التقديرات؟ لقد أسفرت عملية فحص أساليب الأبحاث عن كشف النقاب عن سهولة في التقديرات الزائدة حول حجم الأضرار، فهناك أولا نقص معلومات حول استخدام المعلومات التي كشفت. إن الحالات التي يوجد فيها معلومات صلبة معدودة، في حين أن حجم الأضرار المحتملة واسع. لنفترض أن حاسوبا يحتوي على مجموعة من مخازن المعلومات التي تشمل ألف تسجيل معلومة، ولنفترض أيضا أن مخزن المعلومات ليس مشفرا، والمعلومات المسجلة فيه مكتوبة بلغة طبيعية،وأن كل معلومة مسجلة تمثل بطاقة اعتماد سارية المفعول بجميع التفاصيل المطلوبة لاستخدامه: الرقم ، رقم CVV16 ، سريان مفعولها، الاسم، الهوية وعنوان صاحبها، وتفاصيل حسابات البنك. وفي هذه الحالة يرى اللص صورة كاملة وحقيقية للمعلومات الموجودة في المجموعة. وفي

[16] Card Verification Value الرمز السري المطبوع على الجانب الخلفي من البطاقة. استخدامه يؤكد نفاذ مفعول البطاقة في الحالات التي لا يتم قراءته بالخطوط المغناطيسية.

نفس الوقت فإن المقتحم لا يستطيع أن يقدر القيمة الاقتصادية للمعلومات التي حصل عليها. فهل يستطيع المقتحم أن يقدر بصورة صحيحة القيمة الحقيقية للمعلومات التي سرقها؟ وهل بمقدور الضحية نفسه أن يقدر قيمتها بصورة مناسبة؟ في حالات سرقة الممتلكات الثقافية، ونتائج الأبحاث والتطوير فإن الضحية ينحو نحو تحديد أرباح الحد الأقصى التي كان يسعى إلى تحقيقها في نهاية فترة التطوير، والإنتاج والتسويق بوصفه خسائر عملية السرقة.

إن استخدام الاستطلاعات- وهي طريقة مناسبة لاستيضاح الظواهر التي يصعب مراقبتها واكتشاف تاريخها- هي الطريقة الرئيسية لمعرفة حجم الأضرار. والاستطلاعات تتيح الفرصة للتوصل إلى عدد أكبر وأكثر تنوعا من المستطلعين الذين يقدمون تقديرات خاصة بهم حول كمية الأحداث والأضرار. بيد أن أسلوب الاستطلاع يتسم بنواقص كبيرة تشغل الكثير من علماء الاجتماع والإحصاء.

وثانيا فإن انعدام معلومات كافية يؤدي إلى استخدام أساليب إحصائية من أجل التوصل إلى تقديرات على قواعد تفاصيل معلومات موحدة. إن مشكلة القياس قائمة في جميع مناحي نقاش تهديدات التحكم الآلي، وهي تبرز بصورة خاصة عندما نحاول دعم النقاش بحساب الأضرار بقيم مالية. ولا شك أن هناك صعوبات جوهرية في تقدير الأضرار، ويبدو حتى الآن أن التقديرات المالية الناجمة عن الاستخدام الجامد للأساليب الإحصائية من أجل طرح تخمينات بناء على معطيات ضئيلة، تفضي لتقديرات مبالغ فيها. هناك مشكلة أخرى إضافة إلى مشكلة موثوقية أسلوب الأبحاث، وموثوقية مصادر المعلومات، وملاءمة الأساليب الإحصائية للأبحاث. فالتقديرات المالية تشمل في الغالب عوامل غير مباشر للأضرار. والتقديرات المالية تشمل مساسا بسمعة الشركة التي تعرضت للاقتحام، وتأثيرات سلبية على مسلكية المستهلكين والتي تخلق نتائج اقتصادية صغيرة، وتقديرات أضرار،وتأمين ومصروفات نثرية أخرى.

وهناك قضايا مركزية في فهم هذه الظاهرة بقيت دون إجابة شافية: فهل من المجدي أن نقدر الأضرار بناء على الاستخدام الذي تم عمليات بالمعلومات بدلا من الاحتمال الأقصى؟ هل من الأفضل التطرق إلى القيمة

المالية لتطوير المعلومة بدلا من تقدير ثمنها في السوق حاليا أو مستقبلا؟. وماذا بشأن التكلفة المطلوبة للحماية والعودة إلى العمل بصورة منتظمة؟

نظرة جديدة إلى مغزى جرائم التحكم الآلي:

إذا ألقينا نظرة على جرائم التحكم الآلي، فسوف نجد فيها تعاونا تجاريا مشابها. لقد فتح في غضون السنوات القليلة الماضية سوقا سوداء من الخبراء الفنيين، وأصحاب شبكات حاسوب مأسورة، والتي تطور وتزود من يريد بالوسائل الفنية نظير مقابل نقدي. ويلحق سوق التحكم الآلي الأسود Crime ware as a Service (CaaS) أضرارا اقتصادية جسيمة في الدول المتطورة، ونلاحظ أن المبالغ المالية التي يتداولها هذا السوق تنحو بسرعة وقوة نحو الأعلى.

إن كل من يفضل العمل بقوته الذاتية، وفي نفس الوقت لا يملك موارد أبحاث وتطوير، سرعان ما سيكتشف أن أسلحة التحكم الآلي - مجموعات البرامج الضارة - Toolkits [17]- في متناول أيدي الجميع، وأن بالإمكان تنزيلها من الانترنت نظير مقابل نقدي يتراوح ما بين عشرات وحتى آلاف الدولارات. إن المعلومات هي منتج قابل للتداول، خصوصا وأن إشراكك للآخرين فيما تعرف لا يمس بمقدرتك أو قوتك. وبناء على ذلك ولد وضع جعل المعدات القوية المستخدمة في هذه الحرب متوفرة نظير مقابل هامشي. إن الانطباع القائل أن مجال التحكم الآلي يسهل عملية الكسب المالي عبر الأعمال الإجرامية لم يغب عن أعين المنظمات الإجرامية.

[17] بالإمكان تصنيف أسلحة التحكم الآلي بأنواعها بناء على خاصيتها في الاستخدام على النحو التالي:
*Malware : برنامج ضار مخصص لتشويش العمليات العادية لمنظومة الحاسوب سرا، ومن ثم المساس بالإجراءات التي تقوم بها المنظومة.
* Spyware : برنامج ضار مخصص لجمع المعلومات والمعطيات سرا وأحيانا نقلها عبر الانترنت.
* Scanners: التعرف على مواقع يسهل إصابتها.
* Remote and local Exploits: استغلال موقع مصابة معروفة
* Network Sniffers: التنصت على وسائل الاتصالات.
* Backdoor tools, Trojans: للاتصال عن بعد وإخراج المعلومات.

لقد أتاح نمو قوة الحواسيب،وانتشار شبكة الانترنت وسائل جديدة لتنفيذ جرائم التحكم الآلي بصورة واسعة النطاق: شبكات الحاسوب المأسورة Botnet هي مجموعة شبكات حاسوب شخصية مربوطة مع شبكة الانترنت، وقد زرع فيها برامج ضارة تتيح للمقتحم السيطرة عليها عن بعد دون أن يشوش عملها العادي. إن السيطرة على الحواسيب المرتبطة بالانترنت تجري عبر استغلال ثغرات معروفة لم يكلف المستخدمون وأصحاب الحواسيب أنفسهم عناء معالجتها من أجل إدخال البرامج الضارة. وبناء على العرض ، فإن استخدم Botnet متاح للجميع تقريبا. لقد قدرت شركة (مقافي) عام 2007 أن حوالي 5% من الحواسيب الشخصية المرتبطة بالإنترنت في العالم مأسورة[18].

ومن بين الظواهر الجديدة: Advanced Persistent Threat (APT) أو Adaptive Persistent Attack (APA) – الاستخدام المعقد متعدد المراحل بأسلحة التحكم الآلي لتنفيذ مهام مواصلة وخفية. فالمهاجم لا يعمل على نطاق واسع من أجل استغلال ضعف معروف، بل يحدد الهدف بصورة جيدة، ويستخدم المهاجم سلسلة من الوسائل والمعدات، قسم منها خاص، ومرتبط بالمهمة. ويتألف مثل هذا الهجوم من مراحل عديدة ويمكنها التواصل أشهرا بل ربما سنوات طويلة. ويبدأ المهاجم بجمع معلومات حول البنية التنظيمية للهدف، وتشخيص أصحاب المناصب الرفيعة الذين يتمتعون بتصاريح دخول لغالبية المعلومات. وتتم عملية جمع المعلومات الشخصية باستخدام تفاصيل علنية، وإشراك المعلومات الخاصة في الشبكات الاجتماعية. وبعد اكتشاف الشخصيات المركزية تجري عمليات مركزة للسيطرة عليهم. وإحدى الأساليب التي تستخدم من أجل ذلك هي SpearPhishing - والتي تعني إدخال حصان طروادة عبر البريد الالكتروني، بحيث تحمل الرسالة محتوى موثوقا وفحوى ذات علاقة بالشخص، وتقوم هذه الرسالة باجتياز أجهزة "الترشيح" عبر استخدام المعلومات الشخصية التي تم جمعها، وفتح الرسالة يؤدي إلى زرع حصان طروادة: Remote Access Tool (RAT) جهاز للسيطرة عن بعد على موارد الحوسبة في

McAfee “Virtual criminology report: Organized Crime and the Internet” December 2007[18]

المنظومة عبر خلق اتصال من حاسوب مسيطر في شبكة داخلية. وحال نجاح عملية الاتصال والسيطرة يقوم المجرم بالعمل بسرعة من أجل الحصول على شيء ذي قيمة والتصرف فيه. أما خلال الهجوم عبر APA فإن الأمر يختلف حيث أن التوجه خفي طيلة الوقت مع تجاهل الإغراءات المالية الفورية. فالهجوم يتواصل طيلة الوقت من أجل التغلب على التجهيزات التي تحول دون تواصل تسريب المعلومات. وخلال الهجوم تجري عمليات فحص لاكتشاف رد فعل المنظومات، وفي حالة الضرورة يتم تقسيم المعلومات المسروقة إلى قطع صغيرة مموهة في إطار اتصالات مشروعة، وتمر دون أن تثير شبهة أجهزة الدفاع.

إن الهجمات الموضعية تعتبر أكثر ندرة من الهجمات الإحصائية نظرا لأنها أغلى بكثير: APA يتطلب جمع معلومات استخبارية بصورة منهجية، ومقدرة تخطيط وخبرة، وطول نفس لتنفيذ مهام متواصلة.

وإذا أخذنا الأمر من منظور اقتصادي، سنجد أن هناك وضعا يفيد أنه وعلى صعيد العرض فقد تمكنت مجموعة القراصنة التي نجحت في تطوير وتجسيد برامج للسيطرة على آلاف الحواسيب خلقت في حقيقة الأمر خدمات ذات قيمة اقتصادية كبيرة. أما على صعيد الطلب، فإن زبائن مختلفين - قراصنة آخرين، باحثين خاصين، مجرمين، منظمات تجسس ومنظمات إجرامية كبيرة - عثروا على استخدامات مختلفة لهذه البرامج.

وبناء على ذلك ولد نموذج عمل CaaS سوق العمل السوداء الذي يوجه صناعة خدمات الحاسوب منذ عام 2001. إن الجدوى الاقتصادية للنموذج المذكور واضحة: فمنذ هذه اللحظة لم يعد الزبون مطالبا بشراء تجهيزات حاسوب من أجل استخدام خدمات الحاسوب، حيث أن بمقدوره شراء الخدمة الدقيقة التي يحتاجها فقط من جهات كبيرة واستخدامها في الشبكة ووسائل الاتصالات. لقد اجتاز هذا النموذج الكثير من التحركات خلال السنوات وقد بات حاليا معروفا باسم Buzzword -حوسبة سحاب- Cloud Computing. إن حجم السوق العالمي للحوسبة كخدمات مقدرة ب 14.5 مليار دولار عام 2012.

دعونا نتفحص ظاهرة السوق السوداء من وجهة نظر قومية، إن وجود سوق سوداء لبيع معدات حرب التحكم الآلي، وخدمات تطوير يؤدي إلى انخفاض مستوى الكفاءة التقنية المطلوبة للدخول الى مجال جريمة

التحكم الآلي، لأن المجرم لا يحتاج إلى الاحتفاظ بمقـدرة عـلى تطـوير أجهـزة الاقتحـام وأسـاليب العمـل بنفسـه. أي تطوير البنية التكنولوجية المطلوبة للاختراق والاستخدام غير المشروع بموارد الحاسوب، سواء أكان الاختراق قد خصص من أجل الكسب المادي أو للتخريب. وبذلك يكون قد برز خطر جديـد: إن اسـتخدام المعـدات الموجـودة مـن أجـل التخريب والمساس بالبنى الحيوية بدلا من تنفيذ الأهداف المرتقبة من غش وسرقة إنتاج وتحقيق كسب مـالي سريـع يمكنه أن يلحق أضرارا بالأمن الوطني.

إن تواصل تطور جرائم التحكم الآلي جعل الأمر يتحول إلى مشكلة وطنيـة. إن مسـألة الـدفاع عـن البنـى الحيوية في الدولة هي أهم القضايا في مجال الأمن والتحكم الآلي، ولا شك أن سوق وسائل حرب التحكم الآلي يفـاقم هذه القضايا ويجعلهـا أصـعب، فالمتـاجرة في المقـدرة التقنيـة والتنفيذيـة يمكـن العديـد مـن الجهـات ومـن ضـمنها المنظمات الإرهابية الصغيرة، بل وحتى الأشخاص المنفردين مـن الوصـول إلى مـوارد هائلـة، والتـي يمكـن اسـتخدامها كسلاح تحكم آلي. إن هذا الوضع يشير إلى توسع تهديدات التحكم الآلي إلى مـا يتجـاوز الـدول والمـنظمات الإرهابيـة المعروفة، بل إنها تشمل جميع الجهات القادرة على استخدام الخدمات التجارية التي تعرضها المنظمات الإجراميـة في مجال التحكم الآلي.

إن تخصيص الدول القدر الكافي من الموارد والإمكانيات لأغراض البحث والتطوير المتواصل سيجعل المقدرة التكنولوجية المتوفرة في السوق عاجزة وتلهث خلف التكنولوجيا التي تطورها أذرع الأمن والأكاديميات، وبنـاء عليهـا فإن المعدات والوسائل المتوفرة في السوق ستكون أقل من تلك المتوفرة لدى منظمات الدولة التي تقيم شعب أبحاث وتطوير ذاتية، وتتمتع بدعم من الدولة بالموارد والتنظيم.

توطئة لتجسيد الدولة لمسؤولياتها في مجال التحكم الآلي:

يبـدو البـاحثون وصـانعو السياسـات في حاجـة إلى تفسـير حقيقـي للظـاهرة، فالتقـديرات الماليـة لأضرار الجرائم لا تزودنا بقاعـدة قويـة لفهـم الظـاهرة وبلـورة السياسـات الخاصـة بهـا. وبنـاء عليهـا فـنحن في حاجـة إلى أفضل جداول أولويات إزاء صورة الوضع وتنوع الضرورات والقيود. ودون أن نتفـق عـلى حجـم الضرر المبـاشر وغـير

المباشر الذي تلحقه جرائم التحكم الآلي، فإنه يؤثر على أداء المدنيين، والأعمال والمجتمع. والمدنيون والأعمال الصغيرة تتضرر بأشكال متفاوتة من جرائم التحكم الآلي. فالبريد الالكتروني "القمامة" - البريد غير المرغوب فيه- وخدع الانترنت، وانتحال الشخصيات الرقمية، والمساس بالخصوصيات والابتزاز والتجسس الاقتصادي وسرقة الممتلكات الروحانية والثقافية، كلها ظواهر شائعة، تمس بين الفينة والأخرى بقسم من المدنيين في كافة الطبقات. ورغم أن تقديرات الأضرار تنحو بصورة عامة نحو الأعلى، فإن تطور مجال التحكم الآلي يزيد من حجم المتضررين المحتملين، ويوسع أكثر فأكثر الأساليب التي يمكن استخدامها لتنفيذ جرائم ضد مواطنين وشركات. وعلى ضوء ازدياد حجم المعرفة وفي نفس الوقت توسع الأعمال الإجرامية، يمكننا الافتراض أن المدنيين في الدول المتطورة سيطالبون بأن تتخذ الدولة خطوات وتقوم بعمليات من أجل توفير الأمن الشخصي والجماعي في مجال التحكم الآلي. إن الكشف الإعلامي المتواصل لأحداث حماية المعلومات وهجمات التحكم الآلي تشير بوضوح إلى تفاقم أخطار جرائم التحكم الآلي.

إن الدولة المسؤولة عن قوانين ونظام وأمن مواطنيها مطالبة بالعمل من أجل تقليص الأضرار التي قد تلحق بمواطنيها. وهذه السياسات ستتطور من خلال إدراك المغزى الواسع لهذه الظاهرة وعبر الجدل الجماهيري المثقف والواعي. ونورد فيما يلي مجموعة من القضايا التي تحتاج إلى نقاش جماهير من هذا القبيل.

غالبية الظواهر الشائعة والمندرجة تحت إطار جرائم التحكم الآلي لا تتعلق بقضايا الأمن الوطني. ما مغزى نشر الكراهية وتشجيع التحريض ، ونشر دعاية باستخدام طريقة "البريد الالكتروني القمامة" واختراق الحسابات الشخصية في الشبكات الاجتماعية، وصناعة أفلام وحملات في الشبكة تمس بأحاسيس الجماهير؟ في هذه الحالة سيشعر المواطنون أنهم غير محميين في مجال التحكم الآلي، مما سيمس بكرامة الدولة والكثير من مواطنيها جراء ذلك. أما على المستوى الوطني فإن هذا الضرر هو ضرر طفيف.

ما هو مغزى خداع شائع- سرقة شخصيات رقمية، واستخدام غير مسموح به لوسائل الدفع من أجل سرقة أموال مواطن. عندما يسقط مواطن ضحية لجريمة، فسوف يتوجب على سلطات الدولة أن تعالج هذه

القضية. ولا شك أن بحوزة سلطات الدولة كم واسع من الوسائل والإمكانيات للمعالجة الشخصية،ويجب تمحيص مغزى الأحداث من أجل اختيار السياسة الملائمة للعلاج. أما على صعيد الأمن الوطني، فمن الصعب أن نرى أضرارا على المستوى الوطني طالما أن مستوى الأضرار كان متدنيا نسبيا، حتى لو كانت أعلى في مستواها من مستوى الجرائم التقليدية. ومن الجدير بالذكر أنه كلما ازدادت نشاطات جريمة التحكم الآلي وأصبحت متواصلة على نطاق واسع، فإن ثقة الجماهير في مؤسسات الدولة ستنهار جراء عدم قدرتها على توفير بيئة حماية لها.

إن الوضع الحالي في الدول المتطورة غير مرض. وإذا كان العقد القائم بين الدولة ومواطنيها ينص على "الانصياع مقابل الحماية"، فإن الدولة في هذه الحالة لا تكون قد قامت بدورها في العقد. إن الردود على التحديات الجديدة تتطلب تفاهما واضحا للظواهر ومغزاها، ولا شك أن عمليات الرد وخلق سياسات الفرض والإرغام تتطلب سن قوانين وتشريعات ملائمة، والنشاطات القانونية – التي تلهث بصورة دائمة خلف التطورات الأيديولوجية- تحت حكم الدولة. ويتوجب على أذرع السيادة في الدولة،العاملة وفقا للبنى الشرعية الوطنية تخصيص المزيد من الموارد من أجل الوقاية، والتحقيق والعقاب تجاه جرائم التحكم الآلي.

ورغم الطابع الدولي لمجال التحكم الآلي، إلا أن الدول هي الجهة الاستثنائية التي تتحمل المسؤولية الشخصية للمواطن. إن الاتفاقيات الدولية - مثل "ميثاق بودابست، ميثاق جرائم التحكم الآلي" التابعة لمجلس الاتحاد الأوروبي والمبادرات التي تجري مناقشتها في الأمم المتحدة وفي منظمة الاقتصاد المتطور، وفي اتحاد الاتصالات العالم (ITU)- تعزز التعاون بين السلطات السيادية. والتعاون الدولي يمكنه أن يساعد السلطات ذات السيادة لمحاربة الظاهرة بصورة أفضل، بيد أننا لا نستطيع أن نرى في الاتفاقيات الدولية بديلا للسياسات السيادية المستقلة. ولا شك أن التعاون بين الدول في المنظومات الدولية ممكن إلى حد محدود فقط ووفق مصالحهم المشتركة فقط. ومن الجائز أن الدول الديمقراطية المتطورة ستنجح في بلورة ترتيبات بينها وبين نفسها، لكن الخلافات على صعيد تحديد التهديدات بينها وبين الدولة الدكتاتورية تبدو كبيرة جدا.

يتمحور النقاش الأميركي في هذه القضية حول التجسس الصناعي المتواصل ضد الممتلكات الناجمة عن الأبحاث والتطوير في قطاع التشغيل الحكومي الأميركي. وقد ازدادت مخاوف العديد من الجهات في قطاعات الأعمال الحكومية منذ سنوات كم احتمال فقدان التفوق الاقتصادي الاستراتيجي الأميركي في العالم بوصفها الدولة العظمى العلمية التكنولوجية الرائدة. والحقيقة هي أن مصطلح "فقدان" ليس المصطلح الصحيح الذي يجب أن نذكره، لأن المعرفة لن تضيع، بل ستسرق عبر جهود صينية رسمية منهجية ومنظمة وواسعة النطاق لإبراز قوتها الاقتصادية والعسكرية عبر استنساخ أسرار الأبحاث الأميركية[19]. إن نقاش هذه المسألة يتجاوز المجال الاقتصادي، وحماية المعلومات والمجال القضائي، حتى يصل إلى المجال الأمني الحربي.

والصين من جانبها تنفي هذه التهم نفيا قاطعا، وتبدي قلقا جراء الاستخدام الغربي للانترنت باسم قيم حرية التعبير من أجل تقويض النظام الصيني.

إن السيادة والصلاحيات التي تتمتع بها الدولة داخل أراضيها تمكنها من إنشاء سياسات مستقلة: فسن التشريعات والقوانين وفرضها ليس رهنا بالتسويات الدولية. إن القضية التي تطلق عليها إسرائيل اسم "قضية القرصان السعودي" تعتبر بمثابة نموذج لخروج النقاش من إطار حماية المعلومات إلى المستوى الدولي. ففي مطلع عام 2012 عرف قرصان نفسه باسم OxOmar ونشر على الملأ تفاصيل شخصية وأرقام بطاقات اعتماد لآلاف المواطنين الإسرائيليين[20]. لقد كانت التفاصيل التي تم نشرها بغالبيتها العظمى قديمة، ومن بين 380 ألف تسجيل كانت هناك بضعة آلاف أرقام فقط سارية المفعول. لقد كانت الأضرار التي أصابت أصحاب البطاقات غير ذات بال، حيث قامت شركات البطاقات بإلغائها وصرف بطاقات جديدة وقامت بتغطية أية عملية صرف تمت بصورة غير مشروعة. كما أن حجم المعطيات التي تم الكشف عنها لم يكن غير عادي، ففي كل يوم

---

[19] McConnell, Mike, Michael Chertoff, and William Lynn. “China’s Cyber Thievery Is National policy and Must Be Challenged” The Wall Street Journal, January 2012

[20] روعي جولدبيرج: "بنك إسرائيل: سرقة تفاصيل 15 ألف بطاقة اعتماد" جلوبس 3 كانون الثاني 2012

يتم سرقة ملايين التسجيلات والبطاقات من هذا النوع يوميا من الانترنت .ويتم حزم التفاصيل وفقا لمعايير معينة وبيعها Dumps21 لزبائن في السوق السوداء التي تطرقنا إليها آنفا.

لقد اتضح أن العملية كانت هجوما بسيطا: فقد تمت زراعة spyware في عدة مواقع تجارية إسرائيلية والتي قامت بنقل معلومات كان أصحاب المواقع قد احتفظوا بها دون الحرص على حماية المعلومات. ورغم عدم التعقيد في العملية، وعدم وقوع ضرر حقيقي للمواطنين الذين تعرضوا للهجوم، إلا أن القضية حظيت بتغطية إعلامية واسعة النطاق ومتواصلة لمدة ثلاثة أسابيع، واتسمت في بدايتها بحالة من الرعب. وقد عرضت القضية على أنها عملية تخريبية ضد إسرائيل، لأنه وبدلا من أن يحقق القرصان مكاسب مادية من الاقتحام اختار أن يزرع بدلا من ذلك الرعب بين الإسرائيليين.

ويمكننا تحليل هذه الحادثة بأساليب شتى: حيث يمكننا أن نقول أن المواطنين يفتقرون إلى معرفة حول الحماية، وأن وسائل الإعلام عديمة المسؤولية وتضخم القضايا الهامشية مما يسهم في خلق حالة رعب، وأن أصحاب مواقع الانترنت أهملوا وأجرموا بعدم حماية المعلومات التي جمعوها، وأن الدولة أهملت بخلق بيئة آمنة لتجارة الانترنت وحماية المعطيات الشخصية. لكن في أي تحليل نجد أن علينا أن نعمل على تعزيز الأمن الشخصي والجماعي للمواطنين في مجال التحكم الآلي. وفي نهاية المطاف فإن الطلب موجه إلى الدولة التي تتحمل المسؤولية لأمن مواطنيها. ومن الممكن والمرغوب فيه مناقشة وتحديد الظواهر غير المنطقية والجنائية في مجال التحكم الآلي، ومستويات الأمن المناسبة، وتوزيع المسؤوليات وزيادة معرفة المستخدمين، وحدود تدخل الدولة المطلوب والأزمات الأخرى ذات العلاقة بالقضية.

---

[21] Dump: a stolen credit card or bank accounts and the associated customer data

الفصل السادس

برامج لردع

هجمات التحكم الآلي

- قد تتورط الجيوش الأجنبية في "هجوم على شبكات حاسوب" أو في "استغلال شبكات حاسوب" (CAN\CNE) من أجل الحد أو توجيه ضربة أو تدمير مقدرة دولة أخرى بغية تحسين جداول الأعمال السياسية.

- تقوم المنظمات الإرهابية غير السياسية بتنفيذ عمليات CAN\ANE من أجل تحقيق أجندات سياسية معينة وهي تعزي أهمية كبيرة للإنترنت لأغراض التجنيد والتدريب وجمع المال وتخطيط العمليات.

- تقوم منظمات إجرامية غير سياسية بعمليات سرقة ممتلكات روحانية، وانتحال شخصيات، وأعمال غش وخداع مختلفة، وهم يعملون في الغالب جريا وراء المال.

- الدول التي لا تملك مقدرة خاصة بها لكنها تسعى لإلحاق الضرر بالولايات المتحدة أو حلفائها يمكنها أن تشتري أو تستأجر خدمات المتخصصين من المجرمين والقراصنة لمساعدتهم في تخطيط وتنفيذ هجمات تحكم آلي.

بناء استقرار عبر بناء القوة

تعتبر عمليات الردع في مجال التحكم الآلي - من نواحٍ عديدة- مسألة أشد تعقيدا بكثير من عمليات الردع في الحرب الباردة، وطبيعة مجال التحكم الآلي هي السبب في ذلك. وحتى نظريات الردع النووية التي تعتبر من أشد وأذكى النظريات ستبدو غير مرضية في المواجهة مع تعقيدات هذا المجال، الذي هو من صنع يد الإنسان، والذي يشمل عددا لا نهائي من المقدرة والعناصر والمحركات والحوافز المتغيرة بصورة مستمرة22.

تخلق تهديدات التحكم الآلي مشاكل حقيقية متزيدة، ولم تفلح جميع الجهود التي بذلتها الولايات المتحدة حتى على هذا الصعيد في وضع حد لها. حقا يجب على جميع الجهات أن تعمل من أجل توفير مقدرة رد على مثل هذه الهجمات، بيد أن الولايات المتحدة مثلها كمثل أية دولة أخرى، ستجني فائدة كبيرة إذا نجحت منذ البداية في ردع أعدائها عن العمل، وخصوصا عندما تتعلق العملية بأنواع خطيرة جدا، مثل حرب التحكم الآلي.

لقد بات واضحا تمام الوضوح أن من المستحيل ردع جميع أنواع المسلكيات المعادية، بيد أن من المهم أن نضع جداول أولويات على هذا الصعيد، وتحديد أفضل الطرق لموجهة التهديدات الرئيسة. ورغم الجدل الحثيث الدائر، إلا أن إمكانية بلورة حل شامل وموحد لا زالت بعيدة المنال. ويرجع السبب في ذلك إلى حد كبير للطبيعة المعقدة والشاملة لعملية ردع حرب التحكم الآلي، والذي يتطلب حلولا شاملة ومبلورة تشمل جهات ذات اختصاص واهتمام في القطاعات العامة والخاصة في آن واحد.

وكي نتمكن من بناء النقاش وتحقيق الهدف أو دفعه إلى الأمام، فإننا نقترح إطار عمل يدرس ويمحص القضية بصورة انتقاديه، ترمي للتصدي، ولردع ومنع وإخضاع الجهات المعادية والسياسية وغير السياسية في آن واحد. إن صب التهديدات المحتملة في هذا الإطار الفكري تساعدنا في توضيح مصادر الخطر، وتعتبر بمثابة

---

[22] Eric Sterner, "Deterrence in Cyberspace: Yes, No, Maybe" in Returning to Fundamentals: Deterrence and U.S. National Security in the 21 Century(Washington, DC: George C. Marshall Institute 2011)

نقطة انطلاق لتشخيص المسؤولين وانتماءاتهم للعمليات المعادية التي تجري ضد دولة معينة أو ضد حلفائها. إن هذا الوضع سيتيح الفرصة للاعبين ذوي العلاقة - والذين تحولوا إلى هدف للجهات المعادية – لمواصلة العمل والنقاشات الضرورية من أجل التخطيط والتنفيذ لتطوير وسائل رد فعالة ومناسبة.

هناك ميزة أخرى لهذه الفكرة وهوي تقديم المساعدة في تشخيص مجالات التعاون بين الجهات التي تتعرض للهجمات والتي يمكنها أن تكون مجدية بالنسبة لها أو على الأقل تكون في حاجة إليها.

جهات تشكل دولة:

الجيوش الأجنبية:

قد تتورط الجيوش الأجنبية في "هجوم على شبكات حاسوب" أو في "استغلال شبكات حاسوب" (CAN\CNE) من أجل الحد أو توجيه ضربة أو تدمير مقدرة دولة أخرى بغية تحسين جداول الأعمال السياسية. والجيوش الأجنبية تتشارك المزيد من مقدرة CAN\ANE في الجهود الحربية في التخطيط الحربي والنظريات. هناك تطبيقات تقليدية لمثل هذه الجهود في ميادين القتال – أي تحسين في منظومات الأسلحة أو التشويش على هذه المنظومات من قبل الجهات الأخرى- وكذلك تطبيقات غير تقليدية كلما واصل مجال التحكم الآلي تطوير ميدان القتال وشمل فيه عوامل اجتماعية ومدنية. ومن المتوقع أن يشمل العمل في مجال حرب التحكم الآلي استعدادات استخبارية خاصة بميادين القتال بغية وضع الخرائط للبنى الحيوية للأعداء[23].

أجهزة المخابرات وأجهزة الأمن:

الاستغلال السيئ (Exploit) يمكنه أن يشمل التجسس الصناعي، الاقتصادي، العسكري، السياسي، سرقة المعلومات من حكومات أخرى أو عن حكومات أخرى، وكذلك سرقة ممتلكات روحانية،

---

[23] Siobhan Gorman, "Electricity Grind in U.S. Penetrated By Spies, "Wall Street Journal, April 8, 2009

تكنولوجية، أسرار تجارية وغيره والتي تملكها جهات خاصة أو جامعات. تمارس الكثير من أجهزة المخابرات في العالم التجسس الصناعي بدعم من شركات خاصة[24]. إن الهدف الأساسي من مثل هذه العمليات هي التطلع للتأثير على قرارات وتوازن القوى-الإقليمي والدولي-، وهنا تبرز أهمية الدمج بين المعلومات الاستخبارية الفنية والإنسانية، وكذلك التهديدات من قبل جهات داخلية.

مناحٍ متداخلة:

يمكننا أن ندمج بين العديد من العوامل في إطار قوة الدولة من أجل الحصول على نتائج أفضل. وبمقدور التحالفات بين الدول أن تتبلور لنفس السبب. إن مثل هذه العمليات المشتركة يمكنها أن تشمل جمع معلومات، تعاون بين المعرفة التي يملكها أحد الطرفين وتنفيذ مشترك للعمليات على أرض الواقع – الهجمات. وبمقدور الدول أيضا أن تفتش وتجند جهات غير سياسية، مثل: المخترقين، الذين لا يشعرون بالتزام أو ولاء لأية جهة، واستئجارهم.

جهات ليست دولة:

من المحتمل أن تقوم جهات المنظمات الإرهابية غير السياسية بتنفيذ عمليات CAN\ANE من أجل تحقيق أجندات سياسية معينة. وهي تعزي أهمية كبيرة للإنترنت – لأغراض التجنيد، التدريب، جمع المال، تخطيط العمليات وما شابه-[25]. إن نجاح الجهود التي تبذلها الولايات المتحدة وحليفاتها في الحرب ضد الإرهاب في العالم يمكنها أن تقود منظمات مثل القاعدة وأمثالها للدخول الى عالم التحكم الآلي بصورة أعمق. بل إن من المتوقع أن تحاول القاعدة استقاء العبر من النشاطات التي تقوم بها منظمات "مجهولة" وقراصنة الحاسوب النشطون، أو على الأقل تقليدهم.

منظمات إجرامية غير دولة:

[24] Office of the National Counterintelligence Executive, Foreign Spies Stealing Us Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011

[25] Eben Kaplan, Terrorists and the Internet, Council in Foreign Relations, January 8, 2009

تقوم منظمات إجرامية غير سياسية بعمليات سرقة ممتلكات روحانية، وانتحال شخصيات، وأعمال غش وخداع مختلفة، وهم يعملون في الغالب جريا وراء المال. ومن الجدير بالذكر أن التقنيات والوسائل الخاصة التي تستخدم في حرب التحكم الآلي يمكنها أن تجلب مبالغ مالية هائلة. لقد تم تقدير سوق جرائم التحكم الآلي العالمي بمبلغ 12.5 مليار دولار عام 2011[26]، هذا رغم أن التقديرات تختلف، حيث أن وسائل التقدير تختلف ومن الصعب إثبات أي منها.

مناحٍ متداخلة:

يمكن أن نتوقع تحالفات من قبل جهات غير دولة – منظمات إرهابية، ومنظمات إجرامية، وأشخاص عاديين- بغية جسر الهوة على فوارق المقدرة ومن ثم تحقيق تأثير أكبر. ويمكن أن يحدث ذلك أيضا دولة جهات لا تكون دولة – إرهابيين، مجرمين، قراصنة وأشخاص. وبمقدور الجهات التي لا تشكل دولة أن توسع مقدرة ومهارة الدولة، أو أن تعمل "كرسول" من قبلها لتنفيذ أهداف مختلفة. إن مثل هذه الممارسات تحول تحدي المسؤولية إلى مسألة شديدة التعقيد، ويمكن الدولة من التمتع بإمكانية إنكار موثوق Plausible deniability.

إن المقارنة بين الردع في مجال التحكم الآلي والردع في المجال النووي[27] يبرز نقاط تشابه واختلاف في آن واحد. فمجال التحكم الآلي يتطلب بشكل خاص تركيزا على اللاعبين وليس فقط على مقدرة السلاح. لذا فمن الحيوي تصنيف اللاعبين وفقا لحجم، ولقوة، وطابع التهديد الذي يشكلونه. وبعد أن نقوم بتفحصهم تفحصا دقيقا يمكننا أن نكتشف الأهم من بينهم، والتركيز عليهم بصورة تعطلهم وتعطل نواياهم ومقدرتهم.

إن الدفاع والهجوم مركبان حاسمان في المواقف والإستراتيجية متعددة الطبقات والقوية التي تلجأ إليها الولايات المتحدة، والتي ترمي لحماية الأمن الوطني. والردع يمكنه أن يوفر طبقة دفاعية أخرى عبر منع

[26] Group IB, State and Trends of the Russian Digital Crime Market 2011.
[27] انظرThomas C. Schelling's classic text, Arms and Influence (New Haven: Yale University 1966

مسارات التطوير من قبل أصحاب المصالح المعادية تجاه الولايات المتحدة. لذا فإن الحفاظ على الأمن الوطني وتحسينه يتطلب أن ندرس بصورة جيدة تطوير القدرات كلها -على الصعيدين الدفاعي والهجومي- وضمان أن تصب جميعها في إطار مصلحة الوطن، ومنح الدولة مقدرة النمو والجاهزية للتصدي والردع والإخضاع للخصوم.

ورغم الجهود الحثيثة التي تبذل من أجل تحقيق هذه الأهداف، إلا أنه لا يجب أن نرى في هذا الاتجاه بديلا لبناء وتعزيز وسائل دعم وترميم أخرى تتيح الفرصة لاسترداد الأنفاس بسرعة. ومن الجدير بالذكر أن المقدرة على التعافي واسترداد الأنفاس بسرعة يمكنها أن تكون عامل ردع هائل. ويقول (سون تسو) إن القدرة على التعافي من الضربات، والاستعداد الواضح للرد على هجوم التحكم الآلي، يعملان لتعزيز جهود الردع، مما يحول دون وقوع معارك وسفك دماء. إن القدرة على إخضاع العدو بدون قتال هي قمة النجاح[28].

خطوط هيكلية لتهديدات التحكم الآلي:

تعيش الولايات المتحدة ومصالحها بصورة دائمة تحت تهديدات حرب التحكم الآلي من جهات تشكل دولة وجهات ليست في حكم الدولة، والأهداف الأميركية المحتملة كثيرة ومتنوعة، وتتسع بحيث تشمل قطاعات حيوية كالمياه والطاقة والمال والاتصالات. ويفيد الناطق باسم الإدارة الوطنية للأمن النووي في الولايات المتحدة (MMSA) ، فإن منظمة الأمن النووي الأميركية واجهت عشرة ملايين حدث أمني كبير يومي[29] على صعيد حرب التحكم الآلي. وبناء على حسابات وزارة أمن الوطن الأميركية يتم اكتشاف عشرات آلاف اختراقات التحكم الآلي - محاولات وعمليات فعلية- سنويا، وعشرات آلاف الاعتداءات على منظومات بنى تحتية حيوية -وقد شهدت الفترة الواقعة بين 2010 وحتى 2012 ارتفاعا كبيرا. إن عدد المسؤولين الذين ابلغوا عن عمليات اختراق في الماضي والحاضر كبيرة جدا ويشمل نائب الرئيس لشؤون أمن الوطن ومحاربة الإرهاب جون برنر، مدير وكالة الأمن القومي ورئيس هيئة التحكم الآلي الجنرال كايت ألكسندر، ووزير

---

[28] Sun Tzu, The Art of War, translated by Samuel B. Griffith (New York: Oxford University 1963.

[29] Jason Koebler, "U.S. Nukes Face up to 10 Million Cyber Attacks Daily" US News

شؤون الوطن السابق مايكل تشرتوف، والمنسق الوطني السابق لشؤون الأمن ومحاربة الإرهاب ومستشار الرئيس الأميركي الخاص لشؤون حماية التحكم الآلي ريتشارد كلارك.. وقد قدر رئيس المباحث الفدرالية روبرت مولر أن تحل حرب التحكم الآلي في المستقبل بدلا من الإرهاب بوصفه أكبر تهديد على الدولة.

لقد وصف أحد المحللين هذا الوضع بوضوح تام حينما قال: يتواجد العملاء الأجانب والجريمة المنظمة تقريبا داخل كل شبكة شركة أميركية. هناك اتفاق شبه تام في الرأي في أوساط كبار مستشاري الإدارة الأميركية بشأن حماية تفيد أن مجرمي التحكم الآلي أو الإرهابيين العاملين في مجال التحكم الآلي قادرون على شل البنى الحيوية في الدولة في المجال المالي والطاقة والاتصالات".

وإضافة إلى امتصاص الخسائر المالية التي تقدرها سلطة التجسس الوطني المضاد، وجهات أميركية أخرى بالمليارات، فإن استغلال شبكات الحواسيب لسرقة ممتلكات روحانية ذات قيمة كبيرة عبر ثغرات الحماية، جعل الدولة تقف في مواجهة تهديدات كبيرة نظرا لكونها هدفا لجهود الخصوم الساعين للتنقيب فيما يعتبر موازيا على صعيد التحكم الآلي للحصول على معلومات استخبارية في ميادين القتال. وقد حاولت الين وضع خرائط للبنية الأميركية التحتية الحيوية بغية التعامل معها من أجل ردع وإخضاع أي عمل تقوم به الولايات المتحدة.

لقد عانت الصناعات الحيوية في دول أخرى من هجمات التحكم الآلي. فالشركة السعودية أرامكو - وهي شركة حكومية تعتبر من أكبر منتجات النفط في العالم عانت من فيروس من مصادر خارجية أصاب 30000 حاسوب من حواسيبها في آب 2012. وبعد وقت قصير أصيبت شركة RasGas القطرية والتي تعتبر ثاني أكبر شركة لإنتاج الغاز الطبيعي السائل في العالم. وتشير التقارير الصحفية إلى أن الشركة الفرنسية Areva العاملة في مجال محطات الطاقة النووية كانت هدفا لهجوم تحكم آلي في أيلول 2011.

تحتفظ الدول بمقدرة متغيرة على صعيد المستوى والمهارة، وتقوم العشرات منها بالعمل على توسيع مقدرة التحكم الآلي لديها، خصوصا الولايات المتحدة وحليفاتها. وتعتبر الصين بمثابة تهديد دائم ومتقدم على

الولايات المتحدة، رغم أن بصمات الدولة الصينية لا تبدو دائما على شاشة الحواسيب. ومن الجدير بالذكر أن اكتشاف المهاجم يصبح أصعب بشكل خاص حينما تتباعد الفترة الزمنية ما بين الهجوم وبين طلب المساعدة من قبل الضحية[30]. إن النوايا الصينية واضحة منذ عقد تقريبا، ففي سنة 1999 نشر عقيدان في الجيش الصيني كتابا تحت عنوان Unresticted Warfar – حرب غير مكبوحة الجماح- طرحا فيها وسائل بديلة لهزيمة الخصم لا تتمثل في صورة عمليات عسكرية مباشرة وذات طابع تقليدي.

وروسيا أيضا تعتبر بمثابة خصم شديد وذكي في مجال التحكم الآلي. ومن الجدير بالذكر أنه وخلال الحرب التي وقعت بين روسيا وجورجيا عام 2008، هاجمت روسيا شبكة الاتصالات الجيورجية ودمرتها. وقد قال السفير ديفيد سميث: "لقد دمجت روسيا بين عمليات التحكم الآلي والنظريات العسكرية، رغم أنها لم تحرز نجاحا كبيرا. لقد كان الهجوم الذي شنه الروس عام 2008 بمثابة الامتحان الأول للدمج بين النظريات العسكرية وحرب التحكم الآلي. ولا شك أن الجيش الروسي استفاد كثيرا من العبر التي تم استقاؤها منها[31].

لقد تعرضت بنوك والحكومة الأستونية عام 2007 وجهات أخرى أيضا لهجوم حجب خدمات DDOS واسعة النطاق، ومتفرقة ومتواصلة، وغالبيتها من روسيا. لقد نجح القراصنة والمجرمون من مكانهم في روسيا في ترك بصمات أصابعهم. لقد اكتشف المجرمون أن مجال التحكم الآلي هو بمثابة منجم ذهب، وكلما توغلوا في أعماقه كلما حققوا المزيد من الأرباح وكلما وجدوا أن بمقدورهم كسب المزيد. لقد قدر سوق مجرمي التحكم الآلي عام 2011 بأكثر من 12.5 مليار دولار، كان نصيب روسيا منها 2.3 مليار دولار، أي حوالي ضعفه السنة الماضية. كما أن هناك دلائل تشير إلى أن جهات إجرامية منظمة في دول بدأت بالانضمام إلى هذا السوق عبر التعاون في مجال الوسائل والمعطيات من أجل زيادة أرباحها.

---

[30] قال مايكل مككول رئيس اللجنة الفرعية لقضايا الرقابة والتحقيق والإدارة التابعة لمجلس النواب لشؤون أمن الوطن: "إن الصين تقوم بعملية جمع معلومات موسعة جدا حول الاقتصاد والتكنولوجية الأميركية. إن حرب التحكم الآلي التي شنتها الصين والقائمون على أعمال التجسس الذين تستخدمهم هي الأكثر شيوعا في الولايات المتحدة. لقد شكلت الصين مجموعات قراصنة مدنيين والذين تورطوا في أعمال تجسس تحكم آلي، وشكلوا وحدات عسكرية لحرب التحكم الآلي.

[31] David J. Smith, "How Russia Harnesses Cyberwarfare" American Foreign Policy Council Defense Dossie , August 2012

إن احتمالات التعاون في أوساط جهات ذات حوافز وأسباب مختلفة تماما يثير مخاوف جدية، فعلى سبيل المثال الدول التي لا تملك مقدرة خاصة بها لكنها تسعى لإلحاق الضرر بالولايات المتحدة أو حلفائها يمكنها أن تنضم، أو ببساطة أن تشتري أو تستأجر خدمات المتخصصين من المجرمين والقراصنة لمساعدتهم في تخطيط وتنفيذ هجمات تحكم آلي. من السهل أن نعثر على برامج رمزية تحت عنوان: "افعل ذلك بنفسك" من أجل استغلال نقاط ضعف معروفة بل وحتى دودة **Conficker** - والتي لا زالت كامنة، ويمكنها أن تخلق **botnet** - أجهزة كمبيوتر مأسورة- من حوالي **1.7** مليون حاسوب- ويمكن استئجارها للاستخدام. وبناء عليه فإن عدم التمكن من الوصول إلى بنية ما أو عدم الحصول على دعم من دولة كبرى لا يعتبر عائقا. فهناك معرض لأسلحة التحكم الآلي في السوق، والخصوم لم يعودوا في حاجة إلى مقدرة، بل كل ما يحتاجونه هو تحديد اتجاه وتوفر المال اللازم. ولا شك أن من المفزع أن نتذكر أن منظمة القاعدة دعت المجاهدين على شبكة الانترنت لمهاجمة الحكومة الأميركية والبنى الأميركية الحيوية. وقد أشار نائب الأدميرال صموئيل كوكس المسؤول في إدارة التحكم الآلي أن ناشطي منظمة القاعدة يفتشون بصورة نشطة عن وسائل لمهاجمة الشبكات الأميركية عن طريق وسائل الحرب التي يمكنهم شراؤها من القراصنة والمجرمين العاملين في مجال التحكم الآلي. إن مثل هذه التجهيزات والوسائل يمكنها أن تضاعف قوة الحروب التقليدية.

هناك نقاط أخرى تثير القلق على هذا الصعيد، والتي تتجلي بصورة خاصة في كل من كوريا الشمالية وإيران، هاتان الدولتان اللتان تكملان العجز القائم في السوق عبر النوايا التي تبيتها وتعمل لتحقيقها. فإيران تنفق مبالغ كبيرة على توسيع وتعميق مقدرتها على حرب التحكم الآلي[32]. وهي تعتمد منذ فترة طويلة على رسلها من أمثال حزب الله، والذي يباهي بأنه تمكن من إنشاء ما أسماه "تحكم آلي حزب الله" والذي يرمي لتوجيهه لضرب أعدائه. وتشير جهات فرض القانون إلى أن أهداف جهاز التحكم الآلي التابع لحزب الله تشتمل على توجيه وتجنيد فعال لجهاز التحكم الآلي الإيراني. وأن جهاز التحكم الآلي التابع للحزب يقوم بتعليم

---

[32] Yaakov Katz, "Iran Embarks on I> Cyber- Warfare Program" Jerusalem Post December 18, 2011

الآخرين التكتيك الذي يستخدمه محاربو التحكم الآلي. وحزب الـلـه يسارع لاستغلال وسائل الإعلام الاجتماعية مثل فيسبوك، من أجل الحصول على معلومات، الأمر الذي يخلق فرصا أخرى لجمع المزيد من المعطيات، إضافة إلى اكتشاف أهداف محتملة جديدة وتطوير أساليب ملائمة ووسائل وصول إلى الأهداف[33].

لقد قامت جهات من حرس الثورة الإيرانية بمحاولات علنية لجذب القراصنة إليها، وهناك العديد من الأدلة التي تشير إلى أن مجموعة القراصنة السياسية الإجرامية الإيرانيين المسماة Ashiyane تعمل ضمن جهاز التحكم الآلي التابع لحرس الثورة الإيراني. وتقوم شرطة "باسيج" الإيرانية - التي تتلقى مقابلا نقديا نظير كل عملية تحكم آلي تقوم بها – بتوفير الطاقة البشرية للعمل في هذا المجال. وفي حالة نشوب مواجهات في الخليج، ستتمكن إيران من الدمج بين الأساليب المحوسبة والالكترونية لشن هجوم شبكة من أجل المساس بأجهزة رادار الولايات المتحدة وحلفائها، ووضع العراقيل أمامها كي لا تقوم بعمليات دفاعية وهجومية في آن واحد.

وفي إطار محاولة حزب الـلـه تحقيق الردع، أعلن زعيمه حسن نصر الـلـه أنه لن يكون هناك تمييز بين إسرائيل والولايات المتحدة على صعيد الانتقام إذا قامت إسرائيل بمهاجمة إيران من أجل منعها من الحصول على مقدرة نووية. إذا هاجمت إسرائيل إيران، فسوف تتحمل الولايات المتحدة المسؤولية.

ويمكننا القول في الختام أن الدول تستغل مجال التحكم الآلي من أجل إحراز تفوق وتحسين مصالحها بواسطة جمع المعلومات والحصول على كفاءة الهجوم وتوجيه الضربات لمن يبدو لها عدوا. وحتى الجهات التي لا تشكل دولة، المنظمات الإرهابية والإجرامية يعملون على تجيير مجال التحكم الآلي لصالحهم ولتنفيذ أهدافهم، ويستخلصون الفوائد من هذا المجال الذي يقف فيه الجميع على أهبة الاستعداد للعمل، والذي يتيح الفرصة للاعبين المنفردين الكبار والصغار للتأثير بصورة لا تتناسب مع قوتهم وحجمهم. إن عدم التناسب آنف الذكر يخلق بيئة مليئة بالأخطار المختلفة، والتي لم تجذب في السابق انتباه وطاقة الدول العظمى. وبناء عليه،

[33] Cilluffo, Testimony Before the House of Representatives, p. 6

فإن الدول العظمى تخشى من سيناريوهات معينة على غرار تلك التي أشرنا إليها أعلاه، بسبب قدرتها على هز الاستقرار والأمن بل والقضاء عليه نهائيا.

إن هذا التهديد لا يقتصر على الولايات المتحدة فقط، بل يجب أن نأخذ بعين الاعتبار أن هناك جهات أقل تضررا في الحرب الناشبة بين شبكات الحواسيب. ونورد فيما يلي وصف السلطة الوطنية لمكافحة التجسس- وهي الجهة الأميركية التي تجمع بين يديها خيوط محاربة الإرهاب – والتي جاء في تقريرها الذي قدمته للكونجرس للعام 2011: يعتقد المكتب الفدرالي الألماني لحماية القانون أن الشركات الألمانية خسرت مبلغا يتراوح بين 28-71 مليار دولار وحوالي 30-70 ألف مكان عمل سنويا جراء التجسس الاقتصادي الذي تمارسه جهات أجنبية. ومن الجدير بالذكر أن حوالي 70% من الحالات تورطت فيها جهات داخلية.

وتفيد تقارير كوريا الجنوبية أن الخسائر الناجمة عن التجسس الاقتصادي من قبل الجهات الأجنبية عام 2008 وصلت إلى 82 مليار دولار، في الوقت الذي وصلت فيه عام 2004 إلى 26 مليار دولار. ومن الجدير بالذكر أن 60% من الضحايا كانت أعمال صغيرة ومتوسطة، وأن نصف عمليات التجسس الاقتصادي جاءت من الصين.

أجرت وزارة الاقتصاد والتجارة والصناعية اليابانية استطلاعا في أوساط 625 شركة إنتاجية في نهاية عام 2007، ووجدا أن أكثر من 35 % من الشركات المشاركة قدمت تقارير تشير إلى خسائر تكنولوجية. وقد كان الصينيون مسؤولين عن أكثر من 60% من عمليات القرصنة وسرقة المعلومات.

إن التصريحات التي أدلى بها السناتور الفرنسي جان ماري بوكل، والتي وردت في تقرير معلومات لجنة الشيوخ للشؤون الخارجية والدفاع والقوات المسلحة: في فرنسا، تقع السلطات الإدارية،الشركات وأصحاب مكاتب الخدمات الحيوية – طاقة، مواصلات، صحة وما شابه- ضحايا يومية لملايين الهجمات بالتحكم الآلي،ويمكن أن يكون مصادرها قراصنة حاسوب، مجموعات فعالة، منظمات إجرامية وشركات منافسة أو حتى

دول أخرى. وغالبية أصابع الاتهام موجهة إلى الصين أو روسيا، رغم أن مـن الصـعب جـدا اكتشـاف الفعلـة مـن وراء الهجمات.

ويقول جوناثان أفانس – رئيس المخابرات البريطانية: "تضع الإستراتيجية الوطنية البريطانية مسألة حمايـة التحكم الآلي بصورة واضحة إلى جانـب الإرهـاب بصـفته أحـد أربـع تهديـدات رئيسـية تواجههـا بريطانيـا. إن نقـاط الضعف في الانترنت تستغل بصورة عدوانية ليس فقط من قبل المجرمين بل أيضـا مـن قبـل دول، وحجـم الاسـتغلال مذهل: فالأمر يتعلق بحجم صناعي يضم آلاف الأشخاص الذين يقفون خلـف عمليـات التجسـس عـبر الـتحكم الآلي بتمويل من دول وعصابات إجرامية منظمة. تعتقد إحدى كبريات الشركـات اللندنيـة التـي عملنـا معهـا أنهـا خسرت دخولا بقيمة ثمانمائة مليون جنيه إسترليني جراء هجمات التحكم الآلي التي تعرضت لها من قبل دولـة، ولـيس فقـط جراء فقدان ممتلكـات روحانيـة، بـل أيضـا بسـبب المسـاس بتفوقهـا التجـاري خـلال إجـراء المفاوضـات حـول عقـد الاتفاقيات. إن السؤال الذي يطرح نفسه هو: ما العمل؟

ردع هجمات التحكم الآلي والردود متعددة المعايير:

يتوجب على الولايات المتحدة - إزاء الشهادات الكثـيرة المثـيرة للقلـق حـول مقـدرة الـتحكم الآلي والنوايـا العدائية من قبل جهات تشكل دولة وغير دولة في آن واحد- ترسيم وبلورة مسـار تقـدم دقيـق للمواجهـة بقـوة مـع الوقائع والحقائق المثيرة للقلق التي تميز مجال التحكم الآلي حاليا، والتي ليس من المنطقي القول أنها ستختفي قريبا. ولا شك أن من السذاجة القول أن الولايات المتحدة أو حلفاءها قادرون على حل هذه المشكلة بواسطة سور من النار Firewalls فقط. بل يجب على الولايات المتحدة بدلا من ذلك أن توضح وتطبق إستراتيجية لردع اعتداءات الـتحكم الآلي، وأن تساعد بدعم وتعزيز حماية مجال تحكمها الآلي وحمايتها لبناها الحيوية.

هنــاك حــوارات حثيثــة تجــري في العديــد مــن المجــالات، بيــد أنهــا لا زالــت في مهــدها، ونظــرا لأن هذا المجال يتجاوز جميع مناحي الحياة ويختلط بها، فلم يتم حتى الآن بلـورة رد إسـتراتيجي متكامـل.والتهديـدات

تتطور يوميا وتضيف المزيد من التعقيدات رغم وتيرة تيار التهديدات القوي، ورغم أن القطاعات المختلفة لا تتبادل فيما بينها المعلومات حول الوسائل والمعدات التي تستخدمها الجهات المهددة، ولا تعلن عنها.

إن الصمت بصورة عامة ليس مسألة عديمة المنطق، لأن الحكومة تسعى لحماية مواد سرية والصناعات معنية بحماية معلوماتها، لكن على الصعيد العملي، فإن الصمت يعرقل المسيرة التي يجب أن تقدم ردودا رادعة.

وبناء على ما أوردناه آنفا، فإن المهمة تثير الكثير من المخاوف، بيد أن من المتوقع أن تستخلص الولايات المتحدة فائدة من تطوير وتطبيق إستراتيجية لردع التحكم الآلي، ومن الدول التي تتطلع إلى التصدي وردع وإخضاع اعتداءات التحكم الآلي. إن اتخاذ موقف عملية ثابت - أي اتخاذ خطوات حماية أساسية - حماية، دفاع وتكنولوجية- يمكنها أن تشكل 80% من الحل، كما أنها قادرة على تحييد غالبية التهديدات قبل أن تتجسد على أرض الواقع بكاملها.

إن خلق ردع فعال في مواجهة شخص أو جهة ومنعهم من تحقيق أهدافهم، يجب أن ندرك بوضوح هدفهم، وما الذي يسعون إليه. والفكرة تقوم بصورة أساسية على النظرية الإستراتيجية المعروفة التي أرساها مياموتو موساش والقائلة:"اعرف عودك، واعرف سلاحه". إن هذا الفهم الأساسي يشكل الخطوة الأولى على صعيد هزيمة العدو، ومنعه من تنفيذ العملية أو إخضاعه. ولا شك أن تنفيذ النظرية المذكورة رهن بتمحيص الوضع وفهمه من وجهة نظر العدو. حقا أن جميع مصادر التهديد التي أشرنا إليها آنفا تعمل في مجال التجسس واستغلال المعلومات والمنظومات عبر وسائل التحكم الآلي، بيد أنه يتوجب علينا أن نتذكر أن للجهات المختلفة أهدافا مختلفة،وكل طرف يتطلع للحصول على نتائج معينة في عالم الحقيقة، وبناء على ذلك سيقود خطاه.

ترى ما الذي يتوجب على الولايات المتحدة أن تفعله من أجل إقناع جهات في صورة دول للامتناع عن استخدام مخابراتها وجيشها من أجل استغلال شبكات الحاسوب أو للهجوم على شبكات الحاسوب؟ يجب أن يكون رد فعل التحكم الآلي الأميركي ناجما عن إستراتيجية ردع أوسع بكثير من المعطيات المتوفرة، أو بمعنى

آخر أن يكون ردع التحكم الآلي ملائما ومكملا لإستراتيجية الردع الأميركية الأكثر شمولية. ويجب على الدول الأخرى أن تفهم وتقدر حقيقة أن الولايات المتحدة مؤهلة لفرض عقوبات مناسبة إذا تعرضت لاعتداءات تحكم آلي، وأن الرد الأميركي قد يصل في النهاية إلى رد عسكري مع وضع جميع الاحتمالات على طاولة العمل. ويجب على الولايات المتحدة مقابل كل هجوم تتعرض له أن تبدي مقدرة رد بصورة لا تدع مجالا للشك فيما يتعلق بالأبعاد التي ستترتب على اجتياز الخطوط الأميركية الحمراء.

بناء الاستقرار عبر إبراز القوة:

اعتدنا القول أن الهجوم هو أفضل وسائل الدفاع. وبناء على تقارير من مصادر علنية، فإن الولايات المتحدة تعمل على تطوير قواعد للتدخل في كل ما يتعلق بهجمات التحكم الآلي. وتسعى وزارة الدفاع الأميركية لتعزيز ترسانة أسلحة التحكم الآلي التي بحوزتها- هذا رغم أن هجمات التحكم الآلي يمكنها أن تفضي إلى ردود فعل عسكرية أو ردود فعل بالتحكم الآلي. ومثلما أشار نائب رئيس هيئة الأركان المشتركة الأميركية السابق الجنرال جيمس كرتريت والذي قال: إن الجهود والاستثمارات من النوع الذي أشرنا إليه هنا ستساعد في ملاءمة العلاقة بين الدفاع والهجوم والتي كانت حتى الآونة الأخيرة تقف على نسبة 90 -10% لصالح الدفاع. وستعزز وتبني ثقة بمقدرة الولايات المتحدة على ردع أية أعمال عدائية في مال التحكم الآلي بفعالية.

ورغم ذلك فإن جماعات أمن التحكم الآلي في الولايات المتحدة وكذلك في الدول الموازية لها لم تستكمل بعد مساراتها. بل إن الطريق لا زالت طويلة أمامها، وخصوصا في الولايات المتحدة حتى تصل إلى مستوى الكفاءة والنضوج اللذين تبديهما حاليا الجماعات العاملة في مجال حرب الإرهاب في الولايات المتحدة. يعتبر البندان القانونيان رقم 10-50 في القانون الأميركي اللذين دمجا بين عمل المخابرات والجيش بمثابة انفراج كبير في عهد ما بعد الحادي عشر من أيلول، حيث أفضيا إلى إحداث تحسن كبير جدا في الوضع الأميركي العام على صعيد ما أسمي بمحاربة الإرهاب. ولا شك أن بمقدور الولايات المتحدة أن تطبق نفس النظرية على مجال التحكم

الآلي، على أن تأخذ بعين الاعتبار تحديين: تسوية القوانين العاملة على هذا الصعيد، والسعي نحو القيام بمبادرات أكبر.

وكي تتمكن من التقدم في مجال التحكم الآلي عليها هي وحلفائها أن يبدوا مقدرة قيادة ونظرة واسعة إلى جانب وجود مخططات عمل تقوم على أسس صحيحة. لقد حركت الأحداث الإستراتيجية زمنا طويلا، والحقيقة هي أن هذا الوضع تكتيكي تحت غطاء إستراتيجي. فالولايات المتحدة تتمتع بمقدرة متفردة، لكن هذه المقدرة لن تستغل بكاملها قبل أن يتم بلورة إطار إستراتيجي أوسع تصب فيه هذه المقدرة.

وإضافة إلى الأفكار التي طرحت هنا ، هناك عدة مبادئ رئيسية يمكنها أن تصبح قاعدة للتطوير والتطبيق الإستراتيجي من أجل ردع التحكم الآلي المعادي. وهذه المبادئ على النحو التالي:

- المعايرة بغية تحقيق التطلعات: وفي هذه الحالة فإن المقدرة تدعم المصداقية، يجب أن ندرس بحذر عملية المعايرة والفحص القائمتين وتوجيههما كما يجب وفقا للاستثمارات والجهود التي تعكس العلاقة بين الدفاع والهجوم، والتي يمكن لأي اختلال فيها أن يؤثر تأثيرا سلبيا على الأمن القومي.
- البدء والبناء من مركز القوة: إن ردع والتصدي للخصوم بنجاح يتطلب مقدرة على إقناع الأعداء المحتملين بأن الثمن الذي سيدفعونه مقابل العمليات العدائية التي يقومون بها سيكون أكبر من الجدوى التي سيحصلون عليها. لذا فإن تطوير مقدرة على توجيه ضربة افتتاحية والتلويح للخصوم بتلك المقدرة هو أمر ضروري
- التركيز على السرعة والمفاجأة ومقدرة المناورة: يمكننا القول أن أجزاء الثانية في حرب التحكم الآلي يمكنها أن تكون حاسمة. لذا فإن الهدف يتمثل في الرد في الوقت المناسب على قدر الإمكان. وفي الوقت الذي يجب فيه أن يكون واضحا أن هناك عقابا لكل محاولة اعتداء، يجب في نفس الوقت الحفاظ على نوع من الغموض والضبابية فيما يتعلق بطبيعة تلك العقوبات.

- إن التمتع بمقدرة على توجيه الضربة الأولى فقط سيترك الدولة ضعيفة ومعرضة للرد بنفس الصورة إذا كان الخصم قادرا على الرد. وعلى غرار ما حدث على عهد الحرب الباردة النووية، هناك حاجة لإبداء الكثير من الحذر في تفعيل مقدرة توجيه الضربة الثانية التي ستدافع عن القوات وستضمن تفوق الدولة العلمي والتكنولوجي.
- اعرف عدوك: من الجائز أن هذا المصطلح قديم بيد أنه لا زال ساري المفعول، فكي نهزم عدوا محتمل يجب أن نفهمه بصورة عميقة ونعرف أهدافه وتطلعاته كي نتمكن من بناء الإستراتيجية والتكتيك وملاءمة الوسائل التي نملكها للخصم ومواجهته. والقاعدة المعمول بها هنا هي: انظر، توجه، قرر واعمل (Observe, orient, decide and act).

الفصل السابع

نظرة على التحديات

الأمنية في عهد المعلومات

- تتعلق حرب المعلومات بعدة مناحي مختلفة: حرب الحواسيب والحرب الالكترونية والحرب النفسية ومعالجة وسائل الاتصالات.

- إن النتائج المباشرة التي أسفرت عنها "الثورة في المناحي العسكرية، هي التفوق العسكري التام لجيوش الدول المتطورة في ساحات المعارك.

- مجال التحكم ليس نتاج صناعة الطبيعة بل هو صناعة يد الإنسان ولم يكن ليقوم دون تكنولوجيا المعلومات التي تم تطويرها في غضون عشرات السنوات الماضية.

- حرب الحواسيب في مجال التحكم الآلي هي بمثابة اختراق غير مسموح به لمنظومات حواسيب الخصم من أجل جمع معلومات استخبارية وتشويش وتضليل ومنع استخدام وتعطيل المعلومات.

مدخل

ألقى التطوير الالكتروني والحوسبة منذ الحرب العالمية الثانية بظله وآثاره على العديد من المجالات وخلق ما نسميه بعهد المعلومات.وهنا نسعى لإبراز العلاقة التبادلية بين تكنولوجيا المعلومات وعهد المعلومات والأمن، وبناء عليه تسلط الأضواء على الظواهر الجديدة. ومن الجدير بالذكر أن قسما كبيرا من ضرورة تطوير عالم الحواسيب يرجع للاحتياجات العسكرية، ومدى تأثير هذا التطوير على الأوضاع الأمنية. بيد أن عهد المعلومات الذي يواصل تطوره بسرعة خارقة وكذلك اتصالات الحاسوب والحاجة إلى الحاسوب في مجالات الحياة حاليا خلق مسألة التحكم الآلي.

ويبدو أن التغييرات تتحدى النظريات القائمة وتتطلب إعادة النظر في المصطلحات الأساسية. ونسعى هنا للإسهام في النقاش الدائر في القضايا الأمنية الناجمة عن تطور تكنولوجية المعلومات. ولا شك أن ضرورة إجراء نقاش عام مثقف، والعمل على بلورة سياسة قاطعة تتعزز بصورة تدريجية على ضوء حقيقة أن الأخطار أصبحت حقيقية. ويكفي أن نشير في هذه العجالة إلى الأحداث التي وقعت في أستونيا عام 2007، وقضية الفيروس ستاكسنت[34]. لقد تضرر طابع الدولة في الحالة الأولى، جراء هجوم بسيط على الصعيد التقني وفي نفس الوقت مكثف على الخدمات القائمة على الانترنت. أما في الحالة الثانية فيبدو أنه تم استخدام سلاح تحكم آلي معقد جدا على الصعيد التقني، والذي تمت بلورته من أجل المساس بشكل خاص بجهاز رقابة عملية صناعية في منشأة محمية لإخصاب الوقود النووي في إيران. لقد اشتملت عملية بلورة السلاح وتفعيله عمليات تمويه طيلة الوقت. ويبدو أن تفعيل سلاح التحكم الآلي المذكور ألحقت أضرارا مادية متراكمة ذات طابع إستراتيجي. وفي الحالات هناك اتفاق واسع على أن دولا هي التي قادت الهجوم، وفي الحالتين لا توجد أية أدلة قاطعة على ذلك. إن فهم الأسس الموضوعة لعهد المعلومات يعتبر حيويا للتعرف على قضية أمن التحكم الآلي.

مقدمة موضوعية:

[34] "The Meaning of Stuxnet: A sophisticated" cyber-missile" highlights the potential and limitations of cyberwar" Economist 397 no. 8702 (2010)

يشغل التغيير التكنولوجي الكثير من المفكرين الذين يبذلون قصارى جهدهم من أجل فهمة ودراسة آثاره الاجتماعية. وهناك ثلاثة مفكرين ذوي علاقة بمحاولة فهم الواقع المتغير. وقد استقينا مصطلح الموجة الثالثة من كتابات الأديبين ألفين وهيدي طوفلر وهما يصفان مرحلة معينة، حيث يقولان: نحن في أوج الانتقال إلى الموجة الثالثة، التي يقوم يها الاقتصاد على المعرفة والسيطرة على المعلومات بدلا من الإنتاج الصناعي الجماعي.

الجدول رقم - 1: الموجات الثلاثة بناء على طوفلر:

	المورد الأساسي	من هو الثري؟	الرمز	وسائل الحرب	طريقة الحرب
الموجة الأولى	زراعة منظمة	صاحب الأرض	موجة	السيف	القتال وجها لوجه على بعد صفر احتلال أرض
الموجة الثانية من منتصف القرن 17 وحتى نهاية القرن العشرين	صناعة ممكننة وإنتاج جماعي	الصناعة	آلات إنتاج جماعي	طائرة ودبابة	الحرب بواسطة الآلات على أبعاد متوسطة مع دقة قليلة، ومحاولة للمساس بكفاءة الإنتاج.

الموجة الثالثة منذ نهاية القرن العشرين وما بعده	معرفة	بيل جيتس	حاسوب	حرب تحكم آلي	محاولة للمساس بالمعلومات بوسائل حوسبة، وإلحاق الضرر عن بعد بكفاءة العمل بدون الوصول ماديا إلى الهدف.

لقد تغيرت صورة الحرب أيضا، حيث أن اللعبة ستتمثل في الحصول على معلومات عن العدو ومنعه من الحصول على معلومات. ولا شك أن من سيتمكن من السيطرة على تكنولوجية المعلومات سينتصر في الحرب، حتى لو كان أمامه من سينتج الكثير جدا من معدات الموجة الثانية.

مواجهة المثقفين لعصر المعلومات ي مجال الأمن الوطني:

يعتبر الحاسوب الالكتروني بمثابة رمز عهد المعلومات، وقد تم بناؤه في نهاية الحرب العالمية الثانية من أجل مساعدة الجيش الأميركي في الحسابات البالستية للمدفعية. وفي غضون السنوات الستين التالية، وخصوصا في أعقاب اختراع "الترانزيستور" والدائرة المغلقة، تناقصت معايير الحاسوب بصورة متواصلة، واعتقد جوردون مور - أحد مؤسسي شركة "إينطل" عام 1965 أن عدد الترانزيستورات سيضاعف نفسه في غضون سنة أو سنتين في الرقائق المدموجة في الوقت الذي ستبقى فيه الأسعار ثابتة. وحينما اتضح أن الأمر يسير فعلا على هذا النحو في مجال أنصاف المسرعات أطلق على هذا التوجه اسم "قانون مور". ويقول راي كورتسفيل إنه تم توسيع قانون مور إلى تكنولوجيا المعلومات.

عكفت المؤسسات الأمنية في أعقاب تطور الحاسوب وتصغير حجمه إلى تحسين أداء العديد من المنظومات عبر استخدام الحواسيب، وقد تبدت المساهمة الرئيسية في مجال دقة الذخائر وبدايتها في ذخائر الأسلحة الجوية. لقد أسهمت الحواسيب في البداية في التخطيط للعمليات، وحينما أصبح بالإمكان إدخال حاسوب في الطائرات الحربية، استخدمت عمليات الحوسبة بشكل خاص من أجل أداء المهام الهجومية. وقد طرأ تغيير إستراتيجي حقيقي عندما تضاءل حجم وثمن الحواسيب إلى الدرجة التي أصبح بالإمكان إدخالها في عملية التسليح الذاتية. وهكذا ولد عهد "الأسلحة الذكية"، الأسلحة الموجهة الدقيقة، والتي تم تبنيها في البداية في أسلحة الجو، وقد جاءت النتائج التنفيذية فعالة للغاية. إن ما تستطيع أن تفعله طائرة حاليا باستخدام الأسلحة الذكية في مهاجمة الأهداف الموضعية - كالدبابات مثلا- يساوي أكثر مما كانت خمس عشرة طائرة في سنوات الثلاثينات أو ستون طائرة في سنوات الأربعينات قادرة على فعله، لذا لم يكن من المستغرب أن نقول أن الثورة التكنولوجية أثرت تأثيرا كبيرا جدا، بل حاسما، على نظريات الحرب.

وكي تتم ملاءمة فن الحرب وتكنولوجيا المعلومات، تم في مطلع التسعينات من القرن الماضي تطوير نظرية قتال جديدة تحت اسم "الثورة في المناحي العسكرية" - Revolution in Military Affairs.

RMA . وتقوم هذه النظرية على أربعة أسس: 1- الهجوم الدقيق 2- الفضاء 3- السيطرة على المناورة 4- حرب المعلومات[35].

وتتعلق حرب المعلومات بعدة مناحي مختلفة: حرب الحواسيب – التي تعتبر بمثابة الوسيلة التكنولوجية الأساسية لتخزين ونقل المعلومات- الحرب الالكترونية – وبشكل خاص ضد منظومات الاتصالات. الحرب النفسية، ومعالجة وسائل الاتصالات – بدءا من إطلاع الصحفيين على المعلومات، ومرورا بالصحفيين المندرجين ضمن القوات المقاتلة، وانتهاء بالمعلومات التي يتم إتاحتها للجماهير.

ومن الأهمية بمكان أن نكون دقيقين في المصطلحات وأن ندرك جيدا ما الذي نقصده بمصطلح "حرب المعلومات"، ومثلما سنورد لاحقا فإن هذه المصطلحات تغيرت حال بروز وتطور مجال حرب التحكم الآلي.

إن النتائج المباشرة التي أسفرت عنها "الثورة في المناحي العسكرية"، هي التفوق العسكري التام لجيوش الدول المتطورة في ساحات المعارك[36] ، على غرار ما برز بوضوح خلال الحرب التي خاضتها الولايات المتحدة في العراق وأفغانستان، والحرب الإسرائيلية في لبنان، وضد المنظمات الفلسطينية. وكذلك المقدرة التي لم يسبق لها مثيل على صعيد إدارة حرب "بقوة متدنية" دقيقة وفعالة، بل والقدرة على التغلب على الإرهاب بالوسائل العسكرية دون إلحاق أضرار بيئية واسعة.

إن تطور الحواسيب متواصل مما يتطلب إحداث تغيير متواصل أيضا في النظريات. وسنخصص القسم الباقي من هذه الدراسة لبناء قاعدة لنظرية أمن قومي معدلة في واقع يشمل مجال تحكم آلي جديد.

مجال التحكم الآلي:

خلق الانتشار المتواصل للحوسبة وشبكات الاتصالات في مطلع القرن الحادي والعشرين وضعا جديدا: طبقة محوسبة تمت إضافتها إلى المنظومات القائمة والقديمة، وتمكنت من السيطرة على وظائفها. إن انتشار

---

[35] Michael E. O'Hanlon, Technological Change and the Future of Warfare. Washington, S.C: Brookings Institution Press 2000

[36] التفوق الذي أدى إلى انسحاب الأعداء وأخذهم بإستراتيجية النجاة والحرب غير المتكافئة.

الحواسيب،وتركيبها في أوضاع مختلفة وربطها بشبكات الاتصالات يخلق مجال التحكم الآلي. إن هذا المصطلح يمكننا من فهم ما يحدث في العالم مع التركيز في العلاقة التبادلية مع قضايا ومناحي الأمن الوطني: الشبكات المرتبطة بعلاقات تبادلية لبنى تكنولوجيا المعلومات والتي تشمل شبكات اتصالات، وشبكات ذات أهداف معينة، الانترنت، منظومات حاسوب وغيره. وهي تشمل أيضا المعلومات المخزنة، والمصنفة والتي يتم تناقلها بين هذه الشبكات.

ومن الجدير بالذكر أن مجال التحكم على عكس المجالات البرية، البحرية، الجوية والفضائية، فإنه ليس نتاج صناعة الطبيعة، بل هو صناعة يد الإنسان، ولم يكن ليقوم دون تكنولوجيا المعلومات التي تم تطويرها في غضون عشرات السنوات الماضية. إن المعرفة التي تعتبر بمثابة أهم العوامل في مجال التحكم الآلي هي نتاج العمل الإنساني المتراكم. إن بنية وبلورة مجال التحكم الآلي مثلما هو اليوم يخفيان أبعادا وانعكاسات كبيرة على الأمن الوطني.

ويمكننا أن نصف مجال التحكم الآلي بأنه مركب من ثلاث طبقات:

1- الطبقة الملموسة جدا، والتي تستخدم حاليا كبنية لعالم الحاسوب، وهي الطبقة المادية. والمركبات المادية هي أعمدة البناء المحسوسة في مجال التحكم الآلي، وتتسم بمميزات طبيعية: سعة، ارتفاع، عمق، وزن وحجم.

2- الطبقة الثانية، هي المنطق الذي يقوم عليه البرنامج: وهي مجموعة من الأوامر المتنوعة والتي تم تخطيطها على أيدي خبير. ويسيطر البرنامج على العوامل المادية إلى حد كبير، كما أن المعلومات المخزنة في الحاسوب يمكن معالجتها بواسطة أوامر البرنامج، وطبقة البرنامج هي مادية بصورة جزئية، ومنطقية في جزء آخر .

3- الطبقة الثالثة هي مجال التحكم الآلي وهي طبقة المعطيات التي يحتويها الجهاز والتي تقوم بأعمال المعالجة. والمعطيات ومعالجتها تخلق معلومات ومعرفة، وهذه الطبقة هي الطبقة الأقل ملموسة من بين الطبقات الثلاثة، نظرا لأن مميزات المعلومات مختلفة جدا عن مميزات الجوانب المادية العملية.

مميزات مجال التحكم الآلي ونقاط ضعفه:

مميزات	نقاط الضعف
تغييرات بوتيرة سريعة	تقادم سريع للوسائل، بما فيها منظومات الدفاع
بنيةة البروتوكول TCP\IP	من الصعب متابعة الرموز في الشبكة واكتشاف مصادرها.
مستوى تعقيد مرتفع	من الصعب جدا الربط بين الحادثة والنتيجة، ومن الصعب أن نميز بين العطب والهجوم
استخدام واسع النطاق بتجهيزات تجارية قياسية	تقليص فوارق المقدرة بين اللاعبين الكبار والصغار، وإمكانية الإصابة بأضرار ومنظومات تفعيل متماثلة تعرض مجموعة من المنظومات للخطر
معدات الحرب الأساسية رخيصة نسبيا	ثمن الحماية في حالة ارتفاع متزايد.
بيئة قضائية ضبابية	مجال حائر مع فرصة متدنية للعقاب، مما يشجع على عدم الاستقرار

من حرب المعلومات إلى حرب التحكم الآلي:

تعتبر حرب المعلومات في الأدب المهني الأميركي والأوروبي كمميز واضح لعهد المعلومات، ويطلق على حرب المعلومات في المصطلحات العسكرية الأميركية Information Operations والقسم المحوسب منها يطلق عليه اسم Computer Network Operations (CNO) .

إن إلقاء نظرة على الجدول التالي سيكشف لنا النقاب عن أن هذه المسائل هي مسائل كلاسيكية يرجع الاشتغال بها إلى عهد الحرب نفسها. وبمضي السنين تم تطوير عدة أساليب حرب كلاسيكية لحرب المعلومات، بدءا من جمع المعلومات الاستخبارية بواسطة "مجسات" بشرية، وانتهاء بتطوير تكنولوجيا جمع معلومات خاصة – مثل المجسات الحرارية الاستخبارية المنقولة جوا، والأقمار الصناعية وما شابه. وكذلك في مجال الوقاية تم تطوير أساليب كلاسيكية في حرب المعلومات مثل التمويه، التخيل والحجز، التشويش والمنع، الخداع والتضليل والدعاية وغيره.

قضايا مدرجة تحت عنوان حرب المعلومات:

الموضوع	منظومات وتكنولوجية ذات علاقة
جمع معلومات	مجسات مختلفة في جميع أنحاء الطيف الألكترو مغناطيسي
نقل معلومات للمعالجة للمستهلك	وسائل اتصالات واسعة الأفلام، ضغط، تشفير
التخزين والسحب	قاعدة معلومات De-Duplication ، ضغط

معالجة وترشيح معلومات	معالجة رموز رقمية (DSP) رمزية للتشخيص الأتوماتيكي (ATR) مزج معطيات (Data Fusion) ذكاء صناعي (AI)
تقديم معلومات	اتصالات واسعة الأفلام، منظومات عرض وإدارة إنسان – آلة
منع معلومات	إخفاء، تشويش، حرب الكترونية، تشفير، تضليل.
حماية المعلومات	منع الوصول إلى المعلومات من الجهات غير المسموح لها ، تشفير

إن تفحص الجدول أعلاه يقودنا لاستنتاج مفاده أن التجديد الوحيد تقريبا في هذا المجال هو الاتكالية المتزايدة من منظومات المعلومات على الحواسيب. أي أنه وفي الوقت الذي لا تعتبر حرب المعلومات مجال حرب جديد، فإن الأمر ليس على هذا النحو بالنسبة لمنظومات المعلومات المدخلة إلى الحواسيب. إن مجال التحكم الآلي يتيح الفرصة لتحديد أهداف، وأسلحة وأساليب حرب جديدة.إن ما يميز حرب الجيل الثالث – الحرب في عهد المعلومات- ليس حرب المعلومات في حد ذاتها، بل حرب الحواسيب. لذا من المناسب أن نقلص مجال النقاش والتركيز على حرب الحواسيب في مجال التحكم الآلي. إن المستجدات في مجال التحكم الآلي واسعة جدا إلى الحد الذي يجعل من المصطلحات الأساسية مثل: "الحرب، السلاح، الهجوم والدفاع في حاجة إلى إعادة تفسير.

إن حرب الحواسيب في مجال التحكم الآلي هي بمثابة اختراق غير مسموح به لمنظومات حواسيب الخصم من أجل جمع معلومات استخبارية، تشويش، تضليل، منع استخدام، تعطيل المعلومات. هذا في الوقت الذي يجب أن نعمل على منع الخصم من تحقيق إنجازات مماثلة في حواسيبنا. وكذلك فإن الهجمات التقليدية –

كالقصف المدفعي أو الجوي، أو التخريب المادي- لمنظومات حواسيب ستفضي بالتأكيد إلى تشويش ومنع وتعطيل معلومات. لكن الهجوم المادي من هذا القبيل لا يدخل ضمن حرب التحكم الآلي.

إن مميزات مجال التحكم الآلي هي التي تحدد الحرب في هذا المجال. ومميزات مجال التحكم الآلي تجعل من الصعب التمييز بين الهجوم المقصود ووقوع خلل ما، وتضع صعوبات أمام إمكانية أن ننسب عملية ما لجهة ما، لذا تصعب أيضا عملية الرد على الهجوم. وهذه المميزات تعزز مقدرة اللاعبين الهامشيين، وتمنح أولوية للمهاجم على المدافع.

لقد ثار جدل في السنوات القليلة الماضية حول الأضرار التي ولدت جراء حيوية مجال التحكم الآلي لجميع مناحي الحياة في المجتمعات المتطورة. فحرب الحواسيب لا تقتصر فقط على المنظومات العسكرية، فقد أدى انتشار الحواسيب وشبكات الاتصالات لتحويلها إلى جزء من جميع مناحي الحياة. غالبية الشبكات في الاقتصاد المدني مرتبطة حاليا بحواسيب ومرتبطة بمجال التحكم الآلي. ولا شك أن هذه الحقيقة تخلق أضرارا تفتح الطريق أمام الحرب، وتتطلب تقديرات دفاعية من قبل الدول المتطورة.

الهجوم والدفاع في مجال التحكم الآلي:

وسائل حرب التحكم الآلي هي بمثابة "برنامج ضار" أو مواد ضارة والتي تمس بأجهزة حواسيب الضحية وتتسبب في تشويش المعطيات، والتضليل، وحجب الخدمة أو جمع ونقل المعلومات منها. ونقترح هذه الترجمات للمصطلحات الإنجليزية التالية في هذا المجال:

Malware: برنامج ضار خصص لتشويش النشاطات العادية للمنظومات المحوسبة، ومن ثم المساس بالإجراءات المتبعة في هذه المنظومة

Spyware: برنامج ضار مخصص لجمع معطيات سرا وأحيانا نقلها في الشبكة.

Phishing: خدعة تقوم على برنامج وهندسة شركات من أجل الحصول على معطيات لمستخدمين وتفاصيل تتعلق بهم عن طريق الغش.

ويمكن زرع مواد معدنية عبر إضافة مركب ألكتروني آخر لوحدة قائمة، أو إضافة داخل دائرة اندماجية. وبالإمكان القيام بعملية الزرع خلال فترة التطوير، النقل، التفعيل، الصيانة والتعديل[37]. إن استخدام البرامج كسلاح أكثر شيوعا من استخدام المواد المعدنية، فهذه الإمكانية تتيح الفرصة لاستخدام أحدث أساليب الحرب الالكترونية الحديثة. إن المعرفة والتكنولوجية هي منتجات غير متحركة وهنا تكمن أهميتها الكبرى في كل ما يتعلق بحرب المعلومات.

وعندما تثور شكوك حول التعرض لهجوم تحكم آلي، فسوف يكون من الصعب جدا اكتشاف مصدره وهوية المهاجم، فجميع الجهات العاملة في مجال حرب التحكم الآلي تستخدم نفس الوسائل والأساليب، وفي الكثير من الحالات ما يكون هناك تعاون تجاري بين الجهات التقنية ذات المقدرة على شن الهجوم(المبرمجين، مخترقي الحواسيب، وأصحاب الشبكات الأسرة) لأولئك الذين يشترون الخدمات (الباحثين الخاصين، الجريمة المنظمة ومنظمات الاستخبارات). وكي نقول أن هجوم التحكم الآلي هو عمل حربي، يجب أن نلاحظ العوامل التالية:

- **المصدر التنظيمي والجغرافي: هل تقف دولة وراء العملية[38]**
- **الحوافز: هل بالإمكان أن نلاحظ حافزا أيديولوجيا، سياسيا، اقتصاديا، دينيا للهجوم؟**
- **مستوى التعقيد: هل تطلب الهجوم تخطيطا معقدا وموارد كبيرة والتي يمكننا القول أنها متوفرة فقط لجهات تشكل دولة؟**
- **النتائج: هل تسبب الهجوم في إلحاق أضرار وإصابات؟ هل كانت ستلحق أضرارا لولا الأعمال الدفاعية؟.**

---

[37] يقال أن وكالة المخابرات المركزية الأميركية قامت بزرع برنامج مصاب في تجهيزات للرقابة على منظومة نقل غاز اشتراها الاتحاد السوفيتي تسببت في حدوث انفجار هائل في سيبيريا عام 1982.

[38] في أعقاب عملية الحادي عشر من أيلول 2001 انخفض مستوى دعم الدول لحرب التحكم الآلي.

إن طبيعة مجال التحكم الآلي تجعل من الصعب توفير ردود ناجعة لهذه الأسئلة، وخصوصا ردود تتيح الفرصة لتحديد سياسات.

وكي نتمكن من الدفاع عن أنفسنا يجب أن نعرف أننا نتعرض لهجوم، ولا شك أن الأمر ليس سهلا على صعيد التحكم الآلي. وكلما تمكنا من إدخال وسائل الحرب في مرحلة متقدمة، وبشكل خاص قبل بلورة خطة فحص، تصبح إمكانية الاكتشاف أقل. وكلما كان سلاح التحكم الآلي المستخدم أكثر دقة، كلما ألحق قدرا أقل من الأضرار البيئية وقلل إمكانية أن تتمكن الجهة التي تتعرض للهجوم من اكتشافه.

إن عملية الدفاع تتضمن ثلاث دوائر:

1- الاكتشاف: هو نقطة الضعف في هذا المجال، فكيف سنعرف أننا نتعرض لهجوم؟
2- المنع: استخدام الوسائل الكفيلة بوقف المهاجم في مرحلة الاختراق.
3- الرد: تمالك النفس من أجل تقليص إنجازات المهاجم، ووسائل الاكتشاف الجنائية والقيام برد انتقامي.

قضايا مركزية في حرب التحكم الآلي:

إن التغييرات التكنولوجية الرامية لتطوير اقتصاد المعلومات تثير تساؤلات عديدة، وأولها: قضية حماية البنى الحيوية. لقد شهدنا في السنوات الأخيرة نقاشا متطورا حول حماية البنى الحيوية التي ترتكز عليها المجتمعات الحديثة. وقد طرحت التهديدات خلال النقاشات، فعلى سبيل المثال تم تفجير منشأة توليد كهرباء عبر إرسال أوامر التفجير لجهاز الرقابة والسيطرة فيها[39]. ويبدو أن التهديدات تحققت في القضية التي تم اكتشافها في صيف 2010: عندما انتشرت فيروس - دودة - ستاكسنت في حواسيب مفتشا بينها عن حواسيب تستخدم برامج سيطرة ورقابة صناعية من تطوير شركة "سيمنز" من نوع معين، والمربوطة بمراقبة صناعية من نوع معين. وعندما عثرت الدودة على الحواسيب المذكورة، فعلت شيفرة خاصة والتي قامت بدورها

---

[39] التجربة المسماة "أورورا" والتي جرت في المعامل الوطنية الأميركية في منطقة أيداهو.

بتشويش الرقابة المحوسبة مع إخفاء التغييرات عن برنامج الرقابة والقائمين على تفعيل التجهيزات، مما أدى في نهاية المطاف إلى إلحاق أضرار بعملية تشغيل أجهزة الطرد المركزية الخاصة بتخصيب اليورانيوم في إيران. هذا ولم يتم التعرف على مصدر وطول فترة الهجوم.

تعتبر البنى الحيوية للدولة بمثابة هدف مطلوب خلال النزاعات. وإذا كان الأمر على هذا النحو، فلماذا ثارت المخاوف الآن وخصوصا في الدول القوية؟ إن الولايات المتحدة التي تتمتع بأقوى مكانة على صعيد التحكم الآلي هي أكثر الدول التي يثور فيها جدل حول الأضرار. ويرجع السبب في ذلك في الانتقال من حرب المرحلة الثانية إلى حرب المرحلة الثالثة، حرب المعلومات. إن النقاشات المتجددة فيما يتعلق بحماية البنى الحيوية يرجع إلى ظهور تهديدات جديدة لم تكن في السابق قابلة للتنفيذ. إن تطور مجال التحكم الآلي يتيح الفرصة لأول مرة في التاريخ لمهاجمة منظومات البنى الحيوية في مجال التحكم الآلي دون الوصول إلى مكان وجود تلك البنى ودون أن يتم اكتشاف الفاعل خلال الهجوم. ولنفترض انهيار شبكة البنوك في دولة ما في أحد الأيام، ولنفترض أيضا أننا نجحنا في التأكد من أن الأضرار وقعت بسبب هجوم تحكم آلي موجه، ولنفترض أننا نجحنا في اكتشاف الفاعل الموجود في أراضي دولة مجاورة، فهل الهجوم الذي شنه هو هجوم حرب؟ إن الضرر الذي سيصيب تلك الدولة هو ضرر اقتصادي وليس مساسا بحياة الإنسان. وفي الكثير من الأحيان ما تضبط الدول نفسها على الأضرار الاقتصادية التي تلحقها، لكنها لا تضبط نفسها إزاء المساس بحياة مواطنيها[40]. بيد أن الأضرار الاقتصادية يمكنها أن تشل دولة بأكملها.

إن مسألة حماية بنى المعلومات الوطنية الحيوية هي إحدى القضايا المركزية في النقاشات الدائرة حول أمن التحكم الآلي. ولا شك أن هذه المسألة أكبر بكثير من هذا البحث، وتتطلب معالجة خاصة.

إن مصطلح "حرب المعلومات" يثير فورا تفكيرا في مصطلح الحرب نفسه: فهل هجوم التحكم الآلي على المعلومات المحوسبة دون استخدام النيران، هو بمثابة حرب؟ وما هي الأهداف المشروعة في مثل هذه

---

[40] مثلما فعلت إسرائيل في الكثير من الحالات التي قام الفلسطينيون بقصفها بالصواريخ من قطاع غزة، وسقطت تلك الصواريخ في مناطق مفتوحة ولم تلحق إصابات بشرية.

الحرب؟ إن الاستخدام العسكري واسع النطاق للبنى المدنية – وبشكل خاص الاتصالات- يجعل من الصعب أن نفرق بين الهدف العسكري والمدني. فعلى سبيل المثال بنية الحاسوب التابعة لوزارة الدفاع الأميركية مؤلفة من 15000 شبكة وسبعة ملايين جهاز موزعة في جميع أنحاء العالم. بيد أن غالبية اتصالات وزارة الدفاع تجري عبر شبكات مدنية تجارية. وبمقدور المواطنين أن يصبحوا محاربي حاسوب فعالين بصورة لا تقل عن الجنود. فهل يحولهم هذا الوضع إلى هدف محتمل للرد؟ ترى كيف يجب أن نتصرف في حالة وقوع أضرار اقتصادية واسعة النطاق؟ وكيف نحسب هذه الأضرار؟ ولنفترض أن هجوم التحكم الآلي تسبب في عملية تشويش متواصلة في تزويد المواطنين بالكهرباء، وأن إحدى النتائج تمثلت في إطفاء شبكات الإضاءة وإشارات الطرق مما أدى إلى وقوع حوادث طرق وقع خلالها قتلى، فهل يجب أن نتعامل مع ضحايا هذه الحوادث كشهداء حرب تحكم آلي؟ وكيف يجب أن نرد عليها؟ بالنار والمناورات، أو بضربات حرب آلي مضادة؟ إن المشكلة أكثر تعقيدا مما وصفنا، نظرا لأن هجوم التحكم الآلي لا يحتاج إلى قاعدة داخل الدولة، بل ويمكن للمنظمات والأفراد القيام بها. وحرب التحكم الآلي تجري أيضا بين الدول الصديقة في المنافسة على الحصول على معلومات استخبارية دبلوماسية واقتصادية. فهل من المناسب أن نطلق على هذا الوضع حالة حرب؟ وهل من المناسب أن نخوض هذه الحرب في أوقات السلام للأهداف التي أشرنا إليها؟.

إن المشكلة التي تميز حرب التحكم الآلي هي تشخيص المهاجم: فعلى عكس الحروب التقليدية فإن تشخيص المهاجم ومعرفة الأضرار التي ألحقها ليست محتومة في عالم التحكم الآلي. كما لا توجد جبهة محددة تعمل عليه هذه الحرب، والأبعاد الجغرافية لا تعني بالنسبة لهذه الحرب شيئا. كما أن اكتشاف الهجوم ليس مسألة بديهية، حيث أن سمات الحرب والأعطال التي قد تقع لها نفس المميزات. وإزاء هذا الواقع هناك ضرورة لاستثمار مبالغ كبيرة على استعدادات حرب التحكم الآلي وبصورة متواصلة، ويجب أن تشمل عمليات الحماية من تهديدات التحكم الآلي جميع مجالات الهجوم، وأن يتم تطويرها بصورة مستمرة رغم ازدياد الثمن.

إن المزاعم الخاصة بصعوبة الدفاع تشبه إلى حد كبير المزاعم الخاصة بالدفاع الفعال ضد الصواريخ، والمزاعم الخاصة بعدم جدوى الدفاع ضد المخرب المنفرد. ونحن نعتقد أن بالإمكان خلق ردود للتهديدات الجديدة. ولا شك أن لجهات العاملة في مجال الحماية والدفاع ضد هجمات التحكم الآلي تتحمل الكثير جدا من العبء نظرا لأن هناك تفوق للهجوم على الدفاع في هذا الجانب. إن مجال التشفير هو المجال الوحيد في التحكم الآلي الذي يتفوق فيه الدفاع على الهجوم.

وإزاء صعوبة تشخيص الهجوم، ومصدره الجغرافي وهوية المهاجم، نجد أنفسنا في وضع ضبابي يجعل من الصعب الرد، ومن الصعب أن نؤكد شكوكنا. لقد اعتدنا في مجال الأمن التقليدي أن نكرس جهدا كبيرة لقضايا الاستخبارات والإنذار والردع من أجل تقليص الخطوات العدائية. إن مسألة الردع تثير مشاكل كبيرة في مجال حرب التحكم الآلي، ولا يمكنها أن تعمل عملها، نظرا لأن المدافع لا يعرف من هي الجهة التي هاجمته، وهل هي الجهة التي سبق أن قام بمهاجمتها أم لا.

لقد تطورت قوانين كثيرة في إطار الحرب التقليدية، وتمت صياغتها في مواثيق دولية قبل ظهور مجال حرب التحكم الآلي، وهي تعالج القضايا المتعلقة بالحرب المسلحة، والمواجهات المادية، والمساس بالسيادة الإقليمية وما شابه.بيد أن هذه المصطلحات لا علاقة لها بحروب الحاسوب، لذا يجب العمل على تعديلها وملاءمتها لحرب التحكم الآلي. ولا شك أن هذا الاتجاه يتطلب سنوات طويلة قبل أن يتمكن المجتمع الدولي من صياغة القوانين الخاصة به. إن غياب وجود قوانين يجعل من الصعب مواجهة الصدامات اليومية مع مشكلة حرب التحكم الآلي. ولا شك أن القضايا التي استعرضناها في هذه الدراسة ليست قضايا قضائية مجردة، بل هي قضايا سياسية أيضا وتحتاج إلى قرار دولة للقيام بها.

الفصل الثامن

إيران وحرب التحكم الآلي

- فيروس "ستاكسنت" دفع إيران لبذل جهد كبير جدا لتحسين مقدرتها الدفاعية وبناء مقدرة جمع معلومات استخبارية ومقدرة هجومية في مجال حرب التحكم الآلي .

- هدف إيران في مجال الدفاع مزدوج: الرغبة في منع تكرار هجوم عليها مشابه لهجوم ستاكسنت ورغبتها في الحفاظ على وجود النظام الإيراني.

- إستراتيجية حرب التحكم الآلي الإيرانية ترى في هذه الساحة بمثابة ساحة رئيسة على صعيد نظرية الحرب غير المتكافئة والتي تشكل مبدأ أساسيا في نظرية تفعيل القوات الإيرانية.

- إيران قررت استثمار مبلغ مليار دولار لتطوير وشراء تكنولوجيا وتجنيد وتأهيل الخبراء الذين سيعززون مقدرتها الدفاعية والهجومية.

- إيران أنفقت مبالغ كبيرة جدا على مجال السيطرة في مجال التحكم الآلي داخل الدولة ومجال تحرك المعلومات فيها.

مدخل:

يتزايد الإدراك في أوساط الجماهير وصانعي القرارات في العديد من الدول في السنوات الأخيرة حول ضرورة الاهتمام بمجال "حرب التحكم الآلي" بوصفها أصبحت حربا حقيقية. هذا المجال الذي يوفر إمكانيات وعلاجات كثيرة جدا للمهاجمين الراغبين في تشويش منظومات المعلومات والمساس بصورة مادية بمنظومات البنى التحتية الحيوية التي تشرف عليها أجهزة رقابة صناعية. وإزاء هذا الإدراك يتزايد الإنفاق على عمليات بناء القوة في الكثير من الدول بصورة تتيح لها الفرصة للدفاع عن نفسها، وجمع المعلومات، والمقدرة الهجومية زيادة مطردة وواسعة النطاق.

لقد أصيبت إيران بأضرار جسيمة جراء الهجوم عليها بفيروس "ستاكسنت" ذلك الهجوم الذي يمكن أن نصفه كأحد هجمات حرب التحكم الآلي المدمرة، لذا فهي تبذل جهدا كبيرا جدا من أجل تحسين مقدرتها الدفاعية من جانب وبناء مقدرة جمع معلومات استخبارية ومقدرة هجومية في مجال حرب التحكم الآلي من الجانب الآخر.

ومن الجدير بالذكر أن هدف إيران في مجال الدفاع مزدوج: أولا: الرغبة في منع تكرار هجوم عليها مشابه لهجوم ستاكسنت واختراق حواسيبها من أجل جمع المعلومات الاستخبارية مثلما حدث في حالتي الفيروس "دوكو، ولهب". وتشبه النشاطات الإيرانية على هذا الصعيد النشاطات التي تقوم بها الدول الأخرى في العالم والساعية لحماية بناها الحيوية. ثانيا: أما الهدف الثاني فيتعلق بالرغبة في الحفاظ على وجود النظام الإيراني عبر المتابعة ومنع وصول معلومات إلى الجماهير الإيرانية. وفي الكثير من الأحيان تكون وسائل إنجاز هذين الهدفين واحدة، وعلى سبيل المثال: المحاولات الإيرانية لإقامة شبكة اتصالات مختلفة في إيران، أو قطع خدمات "google" في الدولة.

وتعكف إيران من جانب آخر على بناء قوة هجومية، وذلك على افتراض أن استخدام مجال التحكم الآلي في أية مواجهة مستقبلية من أجل تحقيق الأهداف مع الأعداء سيكون حاسما. ومن الجدير بالذكر أن هناك

صعوبات بالغة في جمع المعلومات بصورة علنية حول مقدرة التحكم الآلي الإيرانية، وبشكل خاص فيما يتعلق بمقدرتها الهجومية. لقد وجهت الأضواء في الآونة الأخيرة بصورة دقيقة إلى نشاطات التحكم الآلي التي تقوم بها إيران في أعقاب الشكوك التي أثارتها إيران في عدة مناسبات تحكم آلي خطيرة، ومن ضمنها سرقة أذون الحماية في الانترنت، ومهاجمة الشبكة التنظيمية لشركة النفط السعودية واختراق حواسيب البنك المركزي في الولايات المتحدة.

وتسعى هذه الدراسة إلى طرح صورة آنية حول عدد من العوامل الخاصة بعملية تطوير مقدرة إيران في مجال حرب التحكم الآلي. وسنعمل على تحليل الإستراتيجية الإيرانية في مجال التحكم الآلي في الجزء الأول من هذه الدراسة، أما في الجزء الثاني فسنستعرض الانعكاسات التنظيمية والعملية الإيرانية التي تمت بلورتها لمواجهة هذا الوضع. ثم سنستعرض عدة عمليات تحكم آلي نسبت إلى إيران.

الإستراتيجية الإيرانية في مجال التحكم الآلي:

إن الدور الذي لعبته شبكات الاتصالات والمعلومات في تحريك المظاهرات وحوادث الشغب التي اندلعت في أعقاب الانتخابات الرئاسية في حزيران 2009 في إيران، وأحداث الربيع العربي، وهجمات التحكم الآلي التي شنت ضد إيران، منحت هذا المجال مكانة مركزية في نظرية الأمن الشاملة للنظام الإيراني. ويمكننا أن نلحظ مدى أهمية هذه المجال بالنسبة لصانعي القرار الإيراني بتطرق الزعيم الإيراني خامنئي مباشرة إلى الفرص والأخطار الكامنة في مجال التحكم الآلي حينما أعلن عن إقامة "مجلس التحكم الآلي الأعلى" خلال آذار 2012، وهو المجلس الذي سيتم تشكيله من كبار رجال السلطة، وسيعمل في مجال التخطيط والتطبيق لإستراتيجية عمل موحدة في مجال التحكم الآلي.

إن تحليل النشاطات الإيرانية في مجال التحكم الآلي خلال السنوات الماضية يشير إلى وجود إستراتيجية تحكم آلي إيرانية ذات أهداف واضحة. ومن الجدير بالذكر أن هناك عاملين أساسيين ترتكز عليهما نظرية العمل الإيراني في هذا المجال. ويتعلق العامل الأول بتطوير مقدرة دفاعية في مواجهة الهجمات التي قد

تشنها دول وجهات معادية إلى جانب تطوير مقدرة للعمل في مواجهة معارضي النظام داخليا. أما العامل الثاني، فيتعلق بتطوير مقدرة هجومية تتيح الفرصة لإيران لمواجهة الهجمات فيما يسمى في إيران بالتفوق الأميركي في مجال المقدرة والبنى التحتية في الإنترنت العالمي.

وتعمل إيران على صعيد النظرية الدفاعية لتحقيق هدفين مركزيين، أولا: العمل على تشكيل غطاء تكنولوجي فعال ومتقدم في مجال حرب التحكم الآلي تمكنها من حماية البنى التحتية الحيوية والمعلومات الحساسة من هجمات التحكم الآلي مثل الهجوم الذي شنه الفيروس "ستاكسنت" والذي ألحق أضرارا ببرنامج تخصيب اليورانيوم الإيراني وعطل عملها. ثانيا: تسعى إيران للحفاظ على أكثر من ألف جهاز طرد مركزي في منشأة نتناز النووية، وإحباط هجمات التحكم الآلي التي تقوم بها جهات معارضة ومعارضو النظام، والتي تعتبر مجال التحكم الآلي بمثابة منصة مركزية لوسائل الإعلام، ونشر المعلومات وتنظيم العمليات ضد النظام. كما يسعى النظام الإيراني للحيلولة دون تسلل أفكار غربية ومعلومات تتعارض ومصالحه عبر مجال التحكم الآلي، ومن ثم الحيلولة دون وقوع "ثورة لينة" تمس بمقدرته على السيطرة على الدولة، وباستقراره.

أما على صعيد المقدرة الدفاعية، فتجدر الإشارة إلى ما قيل عن أن الإيرانيين يسعون لبناء شبكة إعلام مستقلة ومنفصلة، صحيح، رغم النفي الرسمي الإيراني.

وفيما يتعلق بالعامل الهجومي، فإن إستراتيجية حرب التحكم الآلي الإيرانية ترى في هذه الساحة بمثابة ساحة رئيسة على صعيد نظرية الحرب غير المتكافئة، والتي تشكل مبدأ أساسيا في نظرية تفعيل القوات الإيرانية. ويعتبر الإيرانيون حرب التحكم الآلي – على غرار الحروب التكتيكية غير المتكافئة الكلاسيكية مثل الحرب ضد الإرهاب وحرب العصابات- بمثابة وسيلة فعالة وعملية تتيح الفرصة لإلحاق أضرار شديدة بالجبهة الخلفية للعدو المتفوق عسكريا وجغرافيا وإستراتيجيا. ويقول خبراء في هذا المجال: أنه في حالة التصعيد في المعركة الدائرة بين إيران والغرب حول الوضع النووي الإيراني، ستعمد إيران لتنفيذ هجمات تحكم آلي ضد البنى المركزية الأميركية مثل: منشآت الطاقة، المؤسسات الاقتصادية، شبكات المواصلات وغيرها.

لقد ألمحت صحيفة "كيهان" الإيرانية الموالية لخامنئي في تموز 2011 إلى هذه النوايا الإيرانية بالقول: "أنـه يجب على الولايات المتحدة توخي الحذر من مهاجمة لاعب غير معروف في مكان ما من العالم على البنى الحيوية".

وإضافة إلى المستوى العسكري الإستراتيجي الإيراني، فإن النظام الإيراني يسـتخدم حـرب الـتحكم الآلي مـن أجل إلحاق الأضرار بنشاطات التحكم الآلي في الدول الغربية وتجـاه معارضـيه في إيـران. وتقـوم مجموعـات قراصـنة انترنت إيرانية - لا علاقة لها بالنظام الإيراني رسميا، بيد أنها تعمل لصالحه - بشن هجمات تحكم آلي متواصلة مثـل: تدمير مواقع انترنت، زرع محتويات موالية لإيران، سرقـة معلومـات، عمليـات تتعلـق بـالاعتمادات الماليـة، وإلحـاق الأضرار بمزودي الانترنت، وتغيير تحركات شبكة الانترنت.

وهناك جانب آخر يمكننا أن نعزيه إلى الصورة الهجومية لإسـتراتيجية الـتحكم الآلي الإيـراني وهـو الجانـب الإعلامي، فالنظام الإيراني يدرك مدى أهمية مجال التحكم الآلي في بلورة النظريات والتطلعات العالميـة للجماهـير في إيران وغيرها، وهو ينفق مبالغ طائلة في خلق جهاز إعلامي كبـير وفعـال قـادر عـلى تعزيـز مكانـة النظـام والمسـاس بأعدائه. وكي تحقق إيران هذه الأهداف الإستراتيجية فإنها تنفق مبالغ لا يستهان بها في خلق نسيج متكامل، ومتميـز ومتعدد الطبقات في مجال الإحباط والتصعيد، والسيطرة، والتحييد، والهجوم في مجال التحكم الآلي.

الصورة التنظيمية والعملية:

كي تـتمكن إيـران مـن تنفيـذ أهـدافها الإسـتراتيجية شرعـت بالعمـل بحـزم مـن أجـل تعزيـز مقـدرتها في مجال التحكم الآلي. وبنـاء عـلى تقـارير عديـدة قـررت إيـران اسـتثمار مبلـغ مليـار دولار لتطـوير وشراء تكنولوجيـا وتجنيد وتأهيـل الخـبراء الـذين سـيعززون مقـدرتها الدفاعيـة والهجوميـة في المجـال: أولا: فـيما يتعلـق ببنـاء بنـى تحتية لتأهيل وتطوير الطاقـة البشريـة في مراكـز الأبحـاث والأكاديميـات. ثانيـا: بـذل جهـود للتطـوير التكنولـوجي

واسع النطاق وفي النهاية بناء القوة التي تشمل تطوير نظرية وبناء منظمات وتسوية صلاحيات العمل من أجل تنفيذ هذه النظرية.

تأهيل وتطوير الطاقة البشرية:

تتمركز بنى التأهيل والتطوير التكنولوجي لمنظومة التحكم الآلي الإيرانية في الجامعات ومراكز التكنولوجيا المنتشرة في أنحاء الدولة. وهناك في إيران شبكة متشعبة من مؤسسات التعليم العالي والأبحاث الأكاديمية العاملة في مجال الأبحاث والتأهيل في مجال تكنولوجيا المعلومات، وهندسة الحواسيب والاتصالات، ويمكننا القول أن الجهة الرائدة على هذا الصعيد هي Sharif of Technology وهي مؤسسة مركزها في طهران قادرة على منح شهادات أكاديمية في هندسة الحاسوب والالكترونيات، وهي تقيم معهدي أبحاث في مجال التكنولوجية والرياضيات: Advanced Information and Communication Technology Center لعلوم الاتصالات والرياضيات. و Advanced Communication Research Institute .

أما على صعيد كل ما يتعلق بمجال أمن المعلومات، فهناك Amirkabir university of Technology ومقر هذه الجامعة في طهران، وهي تستخدم شعبة للرياضيات وعلوم الحاسوب،وشعبة لهندسة الحاسوب وتكنولوجيا المعلومات. ويبدو أن تقدما حدث في هذه الجامعة على صعيد حماية المعلومات، حيث تقدم شعبة هندسة الحاسوب عدة دورات متقدمة في أمن المعلومات، وتستخدم معمل أبحاث متخصصا في الحماية، ومعملا لتحليل الشبكات المحمية.

وإضافة إلى الأبحاث والتأهيل في المؤسسات الأكاديمية تنفق السلطات الإيرانية مبالغ طائلة في تحسين ودعم الشركات العاملة في مجال التكنولوجيا وخصوصا تلك العاملة في مجال تكنولوجيا المعلومات واتصالات الحاسوب.والاستثمار الإيراني يجري بصورة مباشرة - عبر جهات حكومية مثل وزارة العلوم - وعبر التمويل وإنشاء المعامل لمساعدة شركات التكنولوجيا التي تهتم بها السلطات الإيرانية.

ومـن ضـمن الجهـات الحكوميـة المركزيـة في كـل مـا يتعلـق بتكنولوجيـا المعلومـات، هـو معهـد: Iran Telecommunications Research Center وهـو معهـد متخصـص في مجـال تكنولوجيـا المعلومـات والاتصـالات ويعتبر بمثابة ذراع الأبحاث المترفة في وزارة المعلومات والاتصالات. ويقوم هذا المعهد بتفعيل وتأهيل طواقم أبحـاث متقدمة مختلفة ومن ضمنها أبحاث المعلومات.

وهنـاك جهـة حكوميـة أخـرى تعمـل في مجـال الأبحـاث وتكنولوجيـا المعلومـات وهـو: Technology Cooperation Office (TCO) والذي يعتبر تابعا لمكتب الرئيس، وهدفه المعلن هو تحسـين التعـاون التكنولـوجي مع الدول الأخرى. وهذه المؤسسـة توجـه وتبـادر إلى بنـاء مشروعـات أبحـاث في العديـد مـن المجـالات ومـن بينهـا تكنولوجيا المعلومات. وقد اعتبر الاتحاد الأوروبي وجهات أخرى في الغرب هذه المؤسسة متورطة في البرنـامج النـووي الإيراني.

وإضافة إلى الإنفاق المباشر من قبل الجهات الحكومية، يقـوم النظـام الإيـراني بتفعيـل بـرامج تكنولوجيـة تجري فيها أبحاث في مجال حماية المعلومات، ومن بين المراكز العاملة في هذا المجـال Paradis Technology Park والذي يطلق عليه اسم "عمق السيلكون الإيراني". لقد أقيم هذا المجمع التكنولوجي عام 2001 بمبـادرة مـن مكتـب الرئيس،ويعمل فيه أكثر من أربعين شركة في مجال تكنولوجيا الاتصالات والمعلومات. أما مجمع التكنولوجيا الآخر فهو Guilan Science and Technology Park والذي يعتبر بمثابة مركز دعم للشركات في بدايـة طريقهـا، وتعمـل فيـه عدة شركات في مجال حماية المعلومات.

التعاظم التكنولوجي:

إضـافة إلى تطـوير وإعـداد منظومـات حـرب الـتحكم الآلي القويـة عملـت إيـران في المجـال التكنولـوجي مـن أجـل خدمـة أهـدافها الإسـتراتيجية في سـاحة حـرب الـتحكم الآلي. وقـد أنفقـت إيـران مبـالغ كبـيرة جـدا عـلى مجال السيطرة في مجال التحكم الآلي داخل الدولة ومجال تحرك المعلومات فيهـا. لقـد طـور النظـام الإيـراني خـلال

السنوات القليلة الماضية منظومات تكنولوجية حديثة تتيح له إمكانية متابعة ومراقبة حركة المعلومات في شبكات الحواسيب وأجهزة الهواتف الخليوية في الدولة.

لقد اشترت شركة الاتصالات Telecommunication Co. of Iran والتي تعتبر أكبر شركات الاتصالات الإيرانية الحكومية، من شركة ZTE Ciro الصينية منظومة متابعة قادرة على رصد المعلومات في خطوط الهواتف، وشبكات الحاسوب وخطوط الهواتف الخليوية. وقد اشترى الإيرانيون هذه المنظومة كجزء من صفقة شاملة بين الشركتين اللتين تبلغ قيمتهما المالية حوالي 130 مليون دولار. وقد تضمنت الصفقة منتجات من منظومة ZMXT. إن المنتجات التي اشترتها إيران تمكنها من وقف عمليات السماع، وإرسال رسائل والدخول إلى الانترنت.

وإضافة إلى مراقبة المعلومات، فقد عملت السلطات الإيرانية لتطوير تكنولوجيا لحجب وترشيح مواقع. ونظرا لأن العقوبات المفروضة على إيران تمنعها من شراء "مرشحات" معلومات غربية، فقد قامت الحكومة الإيرانية بالمبادرة إلى طرح مشروع إيراني داخلي لتطوير تكنولوجيا ترشيح وحجب. وقد قامت شركة Amnafzar للتكنولوجيا – وهي على الصلة بالحكومة الإيرانية- بتطوير تكنولوجيا ترشيح معلومات تسمى SEPAR ،وتقوم هذه التكنولوجيا بتصحيح نفسها بصورة دائمة وتغيير إستراتيجية الترشيح التي تعمل بها بين الفينة والأخرى من أجل تفادى محاولات الالتفات عليها. وقد نجح النظام الإيراني باستخدام هذه التكنولوجيا في الحد جدا من تدفق المعلومات في الدولة وإليها.

لقد أشار البحث Open Net Initiative - والذي جرى كمبادرة مشتركة من عدة مؤسسات ومن بينها جامعتي هارفارد وتورنتو، ونشر في آذار 2009- إلى أن إيران هي إحدى الدول الرائدة في العالم في مجال ترشيح وحجت المواقع إلى جانب دول أخرى مثل: الصين، كوريا الشمالية، سورية وميانمار.

إن هذه التكنولوجيا تمنح إيران سيطرة وطيدة نسبيا في مجال التحكم الآلي داخل الدولة، هذا رغم أن النظام يتطلع إلى السيطرة المطلقة على المعلومات ، وكي يتمكن النظام من تحقيق هذه السيطرة طورت إيران

مشروع بناء شبكة إنترنت قومية مستقلة منفصلة عن شبكة الانترنت العالمية. ويعتقد النظام الإيراني أن بناء شبكة الانترنت المستقلة المسماة "هالال" ستمكنه من السيطرة الكاملة على البرامج والمحتويات التي يمكن للجماهير أن تتعرض لها، والمساس بمعارضي النظام بصورة شديدة نظرا لأن قسما كبيرا من نشاطاتهم تجري عبر الشبكة، وتقليص إمكانية إدخال فيروس وتنفيذ عمليات هجومية للتحكم الآلي على البنى الإيرانية. لقد بدأ هذا المشروع يتبلور عام 2009 عندما أمرت السلطات الإيرانية الشركات الإيرانية بنقل نشاطاتها من شبكة الانترنت الدولية إلى شبكة الانترنت ومراكز المعلومات العاملة داخل الدولة.

وقد أفادت التقارير عام 2012 أن إيران تعمل على تطوير شبكة بريد الكتروني داخلي، ومنظومة تفعيل ذاتية، ومحرك بحث ووسائل أخرى للعمل في الشبكة القومية الجديدة. وفي آب الماضي أعلن وزير الاتصالات الإيراني رضا طهبور أن إيران ستنفصل عن شبكة الإنترنت العالمية في غضون ثمانية عشر شهرا، ورغم ذلك يقول خبراء غربيون أن النظام الإيراني سيجد صعوبة في الانفصال بصورة كاملة عن الشبكة العالمية.

تسعى إيران لتنفيذ إستراتيجية عزل الشبكات، بما فيها في القطاعات الأمنية وإنشاء شبكة اتصالات استخبارية قومية مفصولة عن الشبكة الدولية. لقد بدت بوادر هذا الاتجاه في شبكة الاتصالات الداخلية التابعة لحرس الثورة الإيراني Basir والتي تم الكشف عنها في آذار 2012. وتصفها التقارير بأنها نوع من أنواع شبكات الأجهزة الخلوية المغلقة والتي من الجائز أن يتم تفعيلها من محطات إرسال مخصوصة. ومن المفروض أن تزود هذه الشبكة حرس الثورة بخطوط اتصالا مشفرة وفعالة حتى في حالات تعرض شبكات الاتصالات والمعلومات الإيرانية لهجمات تحكم آلي شاملة. وليس من الواضح فيما إذا كانت هذه الشبكة هي شبكة معلومات أم فقط شبكة صوتية.

بناء القوة:

لقد مكن جهاز التأهيل والتطوير الإيراني الواسع مكنها من إقامة جهاز تحكم آلي واسع وذي كفاءة ومقدرة متنوعة على الصعيدين الدفاعي والهجومي. لقد شرعت إيران في العقد الأخير بخطوة إستراتيجية

لتوسيع جهاز التحكم الآلي القومي، فأنشأت وكالات وجهات تحكم آلي في كل جهة حكومية ذات علاقة بالتحكم الآلي. وترمي إيران من هذه الخطوات إلى بلورة منظومة تنظيمية للتحكم الآلي متدرجة الإدارة، ومتنوعة وذات إستراتيجية عمل واضحة، وتخصيص موارد بصورة يجري التخطيط لها، وتوزيع مجالات المسؤولية ومقدرة الحماية وتوزيع المعلومات والمعرفة.

لقد بلغ الإيرانيون ذروة التعاظم في مجال التحكم الآلي – مثلما أوردنا آنفا- حينما أنشأوا "المجلس الأعلى لمجال التحكم الآلي" في آذار 2012 بأمر من الزعيم الأعلى خامنئي، والذي يعتبر بمثابة الصلاحية العليا في الدولة في كل ما يتعلق بمجال التحكم الآلي. ويترأس الرئيس الإيراني هذا المجلس،ومن ضمن أعضائه شخصيات رفيعة مثل قائد حرس الثورة، ورئيس المجلس، ووزراء العلوم، والاتصالات والمواصلات، وقائد الشرطة، ورئيس منظمة الدعاية الإسلامية. ويتمتع المجلس بصلاحية تحديد سياسة التحكم الآلي القومية، والتوجيهات التي يقرها ملزمة لجميع الجهات الإيرانية العاملة في هذا المجال. ويجري التخطيط لإنشاء "مركز تحكم آلي قومي" خاضع للمجلس ويضم جميع نشاطات وعمليات التحكم الآلي الإيرانية، ويركّز ويوزع المعلومات والتوجيهات ويشرف على تنفيذ أوامر المجلس من قبل جميع الجهات ذات العلاقة.

يتركب جهاز التحكم الآلي الإيراني من عدد كبير من منظمات التحكم الآلي التي تنتمي بصورة رسمية لجهات رسمية مختلفة وتعمل في العديد من المجالات. وهناك منظمة مركزية ذات اتجاهات حماية في تركيبتها وهي "قيادة حماية التحكم الآلي"، والتي تعمل تحت رعاية "منظمة الحماية السلبية الإيرانية" الخاضعة لهيئة الأركان العامة الإيرانية. وإلى جانب رجال الجيش يعمل في هذه المنظمة ممثلون وأعضاء في وزارات حكومية، مثل وزارات الاتصالات، الدفاع، المخابرات والصناعة، وهدفها المركزي تطوير نظرية حماية شاملة للمؤسسات والبنى التحتية في الدولة ضد هجمات وتهديدات التحكم الآلي. وهذه المنظمة هي منظمة حماية بصورة أساسية، ولم تكن هناك أية أدلة حتى اليوم تشير إلى أنها عملت في مجال هجوم التحكم الآلي.

وهناك جهات تحكم آلي دفاعية إيرانية أخرى، هي مركز حماية المعلومات MAHER والذي أنشئ ويعمل تحت إشراف وزارة الاتصالات وتكنولوجيا المعلومات. والمركز مسؤول قبل كل شيء عن تفعيل طواقم رد سريع Computer Security Incident Response Teams في حالات الطوارئ وتعرض إيران لهجمات تحكم آلي. كما يقوم المركز بتأهيل الطاقة البشرية المتميزة، وتطوير أساليب عمل لمعالجة أزمات التحكم الآلي، كما يعتبر مركزا لتخزين وتوزيع المعلومات في مجال حماية المعلومات. والمركز مسؤول عن حماية جميع مواقع الانترنت الحكومية، وكذلك مواقع الشركات الخاصة العاملة بصورة رسمية ومسجلة في وزارة الاتصالات. ومن الجدير بالذكر أنه تم تفعيل طواقم هذا المركز من أجل التصدي وإحباط نشاطات البرامج التي هاجمت إيران "ستاكسنت وفلام".

وتعمل منظمات تحكم آلي أخرى في إيران، وتمحور عملها حول السيطرة وفرض الأوامر على أجهزة التحكم الآلي الإيرانية الداخلية التي تتعارض ومصالح النظام. وفي تموز 2009 أنشأ "المجلس الأعلى للثورة الثقافية" الخاضع للزعيم الأعلى "لجنة تشخيص المواقع غير المرخصة". وتضم اللجنة في عضويتها النائب العام، قائد الشرطة، رئيس وسائل الإعلام الحكومية، ووزراء حكومة مختلفين – المخابرات، الاتصالات، الثقافة والعلوم وغيرها- ومن مهام هذه اللجنة العمل على اكتشاف مواقع الانترنت التي لا تتساوق برامجها ونشاطاتها مع المواصفات المطلوبة من النظام. ويحق للجنة أن تأمر بحجب الوصول إلى هذه المواقع.

ومن الجدير بالذكر أن إيران أنشأت عام 2011 وحدة تحكم آلي تابعة للشرطة FETA، ويتمثل هدف هذه الوحدة في مواجهة جرائم الانترنت:الغش، سرقة المعلومات، التهديدات وما شابه، ومن ضمن صلاحياتها أيضا أن تعمل ضد الجرائم السياسية والأمنية في مجال التحكم الآلي،وهي المهمة التي تعتبر على الصعيد العملي أساس نشاطاتها.

وإذا أخذنا مسألة المقدرة الإيرانية الهجومية في مجال التحكم الآلي، فسوف نجد أن الصورة أقل شفافية ووضوحا. ويمكننا القول بصورة طبيعية أن حرس الثورة هو اللاعب المركزي في كل ما يتعلق بإقامة

وتفعيل جهاز التحكم الآلي الهجومي. ويقول خبراء التحكم الآلي في الغرب أن مقدرة التحكم الآلي لحرس الثورة تضع إيران بين الدول المتقدمة في العالم في كل ما يتعلق بحرب التحكم الآلي. وتفيد تحليلات وتقديرات مركز الأبحاث Defense Tech لعام 2008 أن جهاز التحكم الآلي لحرس الثورة يستخدم 2400 شخص وتبلغ ميزانيته 76 مليون دولار في تلك الفترة. ويعزي المركز لحرس الثورة مقدرة حرب تحكم آلي مثل: تطوير برامج حاسوب "فيروس" عبر زرع شيفرة في برامج حاسوب مزيفة. تطوير مقدرة حجب لشبكات اتصالات الحاسوب وشبكات Wi- Fi. تطوير شيفرة حاسوب "شريرة" - فيروس وديدان حاسوب- قادرة على نشر نفسها في الشبكات وإلحاق الأضرار بالحواسيب المقصودة. وسائل لاختراق الحواسيب والشبكات من أجل جمع المعلومات الاستخبارية ونقلها لجهات بعيدة، وتطوير أجهزة "نائمة" يتم تركيبها في حواسيب الهدف وتفعيلها بصورة مؤجلة أو حسب الأوامر من أجهزة السيطرة.

وإضافة إلى مقدرة حرب المعلومات يعمل حرس الثورة أيضا لإنشاء منظومة حرب الكترونية ذات مقدرة على حجب أجهزة الرادار ووسائل الاتصالات. وينفق حرس الثورة الكثير على شراء منظومات حرب الكترونية والتي يمكنها أن تشكل بالدمج مع مقدرة حرب التحكم الآلي وسيلة فعالة لإيقاع الأضرار بالأجهزة الالكترونية الأمريكية خلال المواجهات العسكرية. وبناء على بيانات حرس الثورة فقد تجسدت قوة إيران في مجال حرب التحكم الآلي بإسقاط طائرة التجسس الأميركية دون طيار في كانون الأول 2011.

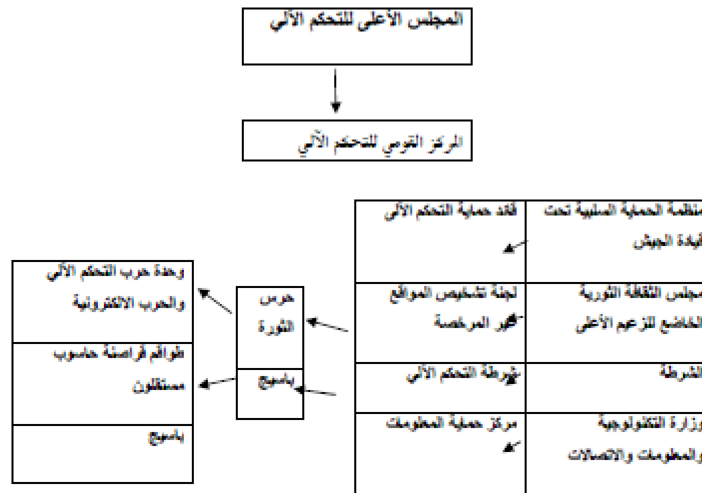
وعدا عن وحدات حرب التحكم الآلي الإيرانية المنظمة، هناك الكثير من الدلائل التي تشير إلى وجود علاقات بين حرس الثورة وبين مجموعات قراصنة حاسوب إيرانيين تعمل ضد أعداء النظام داخل إيران وفي شتى أنحاء العالم. إن استخدام "مصادر خارجية" يتيح الفرصة لحرس الثورة ولإيران الحفاظ على بعد عما يحدث ونفي أية تهم توجه إليها بشأن تورطها في حرب وجرائم التحكم الآلي. . ويعتبر الخبراء مجموعة قراصنة الحاسوب Ashiyane Digital Security Team مجموعة ذات علاقة بحرس الثورة، ويتحرك أعضاء هذه المجموعة بناء على مفاهيم أيديولوجية تؤيد النظام الإيراني والثورة، وتوجه هجماتها ضد أعداء

النظام. وتقوم المجموعة المذكورة بتدريب قراصنة حاسوب، وتمنحهم إمكانية كبيرة يتم استغلالها فيما بعد للعمل السياسي الذي يشمل إسقاط وزرع دعاية موالية لإيران في مواقع غربية وإسرائيلية، وللقيام بارتكاب جرائم تحكم آلي – الغش في شبكات الائتمان، سرقة هويات، واختراق مخازن المعلومات والمؤسسات المالية. وتعقد المجموعة المذكورة هيئة باسم War Games تجري فيها منافسات اختراق بين القراصنة لأهداف شتى ومن بينها شركات بنى تحتية أميركية.

أما مجموعة قراصنة الحاسوب الأخرى التي تعتبر ذات علاقة بحرس الثورة فهي: **Iran's Cyber Army** وهي مركبة من قراصنة وخبراء حاسوب يعملون تحت هوية مصطنعة ويعلنون أنهم ينتمون إلى المجموعة. وتشتمل نشاطات هذه المجموعة على : اختراق المواقع الغربية وزرع محتويات موالية لإيران، السيطرة على نقل المعلومات وإعادة تحويلها من جديد، واختراق شركات حماية المعلومات الغربية وتخريب مواقع معارضي النظام.

وهناك منظمة "الباسيج" الخاصة بحرس الثورة والتي أصبحت ناشطة في مجال حرب التحكم الآلي حال إنشاء "مجلس التحكم الآلي للباسينج" عام 2010. وتتمركز نشاطات الباسينج في خلق دعاية موالية لإيران في مجال التحكم الآلي. وتقوم بتجنيد وتوجيه آلاف الإيرانيين عبر كتابة محتويات ثم تفعيل مجموعات حاسوب منظمة، وعبرها تفعيل عشرات آلاف المواقع المؤيد للنظام ونشر ردود ومواد مؤيدة للسلطة الإيرانية في الشبكات الاجتماعية، والهيئات والمواقع المركزية في إيران وخارجها. وتسعى الباسيج أيضا لتطوير مقدرة حرب تحكم آلي أكثر تطورا وتستخدم موجهين من داخل وحدات التحكم الآلي التابعة لحرس الثورة من أجل تأهيل قراصنة حاسوب ذوي مقدرة هجومية عالية.

ويمكننا القول أن إيران أنشأت خلال السنوات القليلة الماضية منظومة تحكم آلي واسعة النطاق، تشمل مجالات عمل كبيرة وتتمتع بمقدرة متنوعة. والرسم الكاريكاتيري التالي يصف البنية التنظيمية لجهاز التحكم الآلي في إيران مثلما يتضح من التحليل أعلاه:



يمكننا أن نرى التقدم الكبير في تطوير مجال التحكم الآلي في إيران. فعلى الصعيد الدفاعي تعمل إيران بكامل قوتها من أجل خلق مقدرة دفاعية وتفرُّد من أجل مواجهة محاولات الاختراق لشبكاتها وبناها الحيوية. ولا شك أن من الصعب أن نخلق صورة أمينة فيما يتعلق بتطوير المقدرة الهجومية الإيرانية في مجال حرب التحكم الآلي. ويتطرق القسم التالي إلى عدة نشاطات من هذا القبيل.

عمليات التحكم الآلي المنسوبة إلى إيران:

أفضى التحقيق الذي أجرته شبكة التليفزيون **Univision** في كانون الأول **2011** إلى قيام الأميركيين بإجراء تحقيقات بشأن تورط جهات إيرانية رسمية في مؤامرة تحكم آلي ضد الولايات المتحدة. لقد تمكن محققو الشبكة من التسلل إلى داخل مجموعة من قراصنة الحاسوب المكسيكيين كانت تعمل ضد أهداف

أميركية، والتقطوا سرا صورا للقاء بين ممثلي المجموعة وسفير إيران في المكسيك. وقد طرح أعضاء المجموعة فكرة الحصول على دعم وتمويل من الحكومة الإيرانية من أجل القيام بعمليات هجوم تحكم آلي ضد أهداف أميركية ومن بينها وزارة الدفاع، ووكالة المخابرات والمباحث الفدرالية والمنشآت النووية الأميركية. وقد بدا السفير الإيراني في الصور محمد حسن جهادري، وهو يوجه الأسئلة ويقترح طرق عمل محتملة أخرى. وقد أكد أن إيران تسعى للحصول على معلومات استخبارية فيما يتعلق باحتمال قيام الأميركيين بشن هجوم على منشآتها النووية. وفي نهاية المحادثة طالب المجموعة بالحفاظ على الاتصالات ووعد بنقل الاقتراح إلى المسؤولين. ويمكننا الافتراض أن هذه المحاولة لم تكن المحاولة الوحيدة التي تعمل فيها ايران من أجل تجنيد جهات في العالم قادرة على خدمة أهدافها الهجومية في مجال التحكم الآلي.

إن العمل على تحديد الجهة المهاجمة بصورة مؤكدة في مجال حرب التحكم الآلي هي عملية معقدة وتحتاج إلى تخصيص الكثير من الموارد والتعاون الدولي، لذا من الصعب أن نحدد بصورة مؤكدة الجهة التي تقف وراء الكثير من العمليات في هذا المجال. ورغم ذلك بالإمكان في حالات كثيرة وعبر استخدام وسائل تمييز خاصة تحديد الجهة التي تقف وراء الهجمات بصورة شبه مؤكدة.

وسنعمل هنا على تمحيص ثلاث عمليات، الأولى: الهجوم على شركتي حماية بغية سرقة تصاريح حماية في الانترنت. الثانية: تتعلق بهجوم على مؤسسات مالية كبيرة في الولايات المتحدة. والثالثة: شن هجوم على شركة النفط السعودية.

الهجوم على شركتي Comodo ; DigiNotar

تعرضت شركتان تعملان في مجال توفير تصاريح SSL خلال عام 2011 لهجوم تحكم آلي، والشركة الأولى هي شركة Comodo الأميركية، والثانية شركة DigiNatar الهولندية. وقد تعرضت الشركة الأولى للهجوم خلال شهر آذار 2011، وسرقت منها عدة تصاريح من ضمنها تصاريح في مجال domain لخدمات البريد عبر الانترنت مثل Google. لكن الشركة ألغتها قبل أن تقوم الجهة المهاجمة

باستخدامها. ومن الجدير بالذكر أن الجهة التي تحصل على تصريح في مجال mail.google.com يمكنها أن تسرق شعارات Gmail وسرقة حسابات عملاء، وكذلك من يحصل على تصريح مزور في مجال Microsoft.com، حيث يمكنه أن يركب برنامجا شريرا في حواسيب الضحايا. ويتضح من التقرير الذي قدمته الشركة المعطيات التالية:

-يفتقر هذا الهجوم إلى طابع جرائم التحكم الآلي.

-كان المهاجمون منظمين ويعرفون بالضبط ومسبقا ما يريدون، وهو الأمر الذي يشير إلى تورط منظمة تابعة لدولة في الهجوم.

-مصدر الهجوم كان بصورة رئيسية من إيران – بناء على تشخيص عنوان IP.

-مواقع الانترنت التي فحصت فيها التصاريح المسروقة موجودة في إيران، وقد تمت إزالتها عن شبكة الانترنت حال اكتشاف شركة Comodo للهجوم.

لم ينجح الهجوم على الشركة الأميركية في تحقيق أهدافه، وقد تم تشخيص الهجوم ومعالجته قبل أن يقوم المهاجمون باستخدام التصاريح المسروقة. وذلك على عكس الهجوم على الشركة الهولندية. لقد هاجم الفعلة مخازن الشركة التي كانت بمثابة السلطة المركزية في هولندا لتصاريح SSL خلال الفترة الواقعة بين حزيران وآب 2011، وخلال الهجوم الذي أطلقوا عليه اسم " الوردة السوداء" سرقت شهادات تستخدم للتأكد من مواقع بما فيها شهادات تستخدم للتأكد من اسم المجال google.com والتي تسمح للمهاجم بانتحال أسماء مواقع وتوجيه عملاء Gmail إلى الأماكن التي يريدها.

لقد أشار التحليل الذي أجرته الشركة الهولندية – والتي أعلنت إفلاسها بسبب هذه الحادثة ولم تعد قائمة- إلى أنه تمت سرقة 531 شهادة مزورة وأنها استخدمت بشكل خاص من أجل اختراق حسابات البريد الالكتروني للعملاء وبشكل خاص في إيران. وأشار التحليل أيضا إلى أن الهجوم أتاح الفرصة لاختراق أكثر من 300000 حاسوب غالبيتها العظمى في إيران – أكثر من 99%.

ولا شك أن من الصعب الإشارة بصورة مؤكدة إلى مصادر الهجوم، بيد أن الخبراء يقولون إن مصدره في إيران وأنه يأتي في إطار الحاجة إلى الحماية الداخلية. وبشكل خاص للأسباب التالية: أهداف الهجوم وحجم العملاء الكبير الذين تعرضوا للهجوم، البيانات التي تم تركها في موقع الشركة في أعقاب الهجوم والتي دلت على تورط إيراني في الهجوم.

الهجوم على مؤسسات مالية في الولايات المتحدة:

يتضح من التقرير الذي نشر في الولايات المتحدة خلال شهر أيلول 2012 أن عدة مؤسسات مالية أميركية تعرضت لهجوم تحكم آلي قريبا من هذا التاريخ، ومن ضمنها مواقع تعود للبنك المركزي الأميركي، وبنك مرجان تشيس، وبنك سيتيجروب. وتعتقد جهات أميركية أن هجوم التحكم الآلي على المؤسسات المالية الأميركية لم يجر على أيدي قراصنة عاديين، بل أن القراصنة الذين شنوا الهجوم تلقوا تمويلا – على ما يبدو - من قبل إيران، وأن الهجوم يأتي ردا على العقوبات التي فرضتها الولايات المتحدة على إيران .

قام مركز أميركي للتحليل والتعاون في مجال المعلومات المالية بنشر تحذير للبنوك الأميركية فيما يتعلق بهجمات التحكم الآلي والتي ترمي إلى سرقة "هويات" بواسطة البريد الالكتروني، وحصان طروادة ومعدات شريرة أخرى قادرة على استيعاب الدقات على مفاتيح الكتابة، وكل ذلك بغية تخليص أسماء مستخدمين، وعمال وكلمات السر. ورغم أن بنكا كبيرا قد تعرضت للهجوم، فإن غالبية ضحايا الهجمات كانت أعمالا صغيرة ومتوسطة وبنكا صغير وشركات اعتمادات. وقد أعلنت مجموعة تطلق على نفسها اسم " مقاتلو عز الدين القسام للتحكم الآلي" أنها هي التي هاجمت البنك الأميركي "BofA"، وبورصة نيويورك ردا على الفيلم الذي يسيء للنبي محمد والذي نشر في مطلع شهر أيلول 2012.

لقد أشار التحذير من تلك الهجمات إلى أنها تدل على أن المهاجمين نجحوا في الحصول على معلومات كثيرة وإمكانية للوصول إلى شبكات البنوك على الأقل في عدة حالات، كما نجحوا في الحصول على تصاريح دخول من عمال البنك والالتفاف على المنظومات الدفاعية.

هجوم التحكم الآلي على شركة أرامكو:

تعرضت شركة أرامكو السعودية خلال شهر آب 2012 للهجوم - وعلى ما يبدو أن الهجوم تم بمساعدة داخلية من جهة ذات مقدرة عالية على الوصول إلى حواسيب الشركة. وقد تعرض ثلاثين ألف حاسوب تابع للشركة للهجوم. كما تعرضت شركة الغاز القطرية ResGas أيضا لهجوم. وقد تم الهجوم باستخدام فيروس حاسوب يعرف باسم Shamoon . ويقول الخبراء أن هذا الهجوم هو أكثر الهجمات التي وقعت ضد شركة تدميرا. فقد انتشر فيروس الحاسوب عبر باحثي حواسيب الشركة وألحق أضرارا بالمعلومات المحفوظة فيها. ويقول خبراء الشركة أن الأضرار كانت محدودة للحواسيب المكتبية، ولم تؤثر على منظومات التشغيل وأجهزة الرقابة.

لقد اكتشفت شركة سينمتك الفيروس لأول مرة في شهر آب 2012، واتضح من التحليل الذي أجرته الشركة وشركات متخصصة أخرى المعطيات التالية:

1- فيروس Shamoon مخصص لمهاجمة حواسيب في شبكة الحوسبة التنظيمية IT وليس حواسيب منظومات الرقابة. وهذا الفيروس لا ينتمي إلى نظرية وسائل حرب التحكم الآلي الذكية على غرار ستاكسنت الذي هاجم البرنامج النووي الإيراني عام 2010.

2- لم يكن هدف الهجوم الذي شنه الفيروس التجسس أو جمع المعلومات، بل التدمير المطلق للمعطيات وإلحاق أضرار بالحواسيب الهدف.

3- لا يبدو أولئك الذين كتبوا رموز الفيروس من كبار المتخصصين في هذا المجال مثل أولئك الذين كتبوا رمزو "ستاكسنت أو لهباه". بل هناك أدلة تشير إلى أن الجهات التي وقفت خلف هذا الفيروس ليسوا مبرمجين محترفين حيث تم العثور على الكثير من الأخطاء في الرموز، لكنهم كانوا كفؤين على صعيد خلق فيروس مدمر بصورة خاصة.

4- تم إدخال الفيروس إلى حواسيب الشركة بواسطة متعاون من داخل الشركة، وهو أحد الأعضاء الذي له اتصال مباشر مع شبكة الحواسيب في الشركة، وقد قام باستخدام USB من أجل إدخال الفيروس إلى الحواسيب.

5- استخدم كتبة الفيروس قسما من صورة علم أميركي محروق من أجل إخفاء محتوى الأجزاء في الحواسيب المصابة، وهو الأمر الذي يشير إلى انتماء سياسي ديني إسلامي معين.

6- أدخل معدو الفيروس في رمز آلية المحو اسم **Wiper** وهو اسم مشابه للرمز الذي ظهر في الفيروس **Flam** الذي هاجم حواسيب شركة النفط الإيرانية. إن هذه المقارنة تثير شبهات بأن الهجوم الذي شن على شركة أرامكو هو عمل انتقامي كرد على هجوم **Flam**.

لقد أخذت مجموعة تطلق على عاتقها اسم "سيف العدل" مسؤولية الهجوم وزعمت بأن الهجوم يأتي ضد مصدر الدخل الأساسي للمملكة العربية السعودية المتهمة بارتكاب جرائم في دول مثل سورية والبحرين. وأن الفيروس مكنهم من الوصول إلى أسرار كثيرة. لكنهم في الحقيقة لم ينشروا حتى وقتنا هذا أية أسرار من تلك التي أشاروا إليها. إن الهجمات الواسعة التي شنت على شركات نفط وغاز في منطقة الخليج أثارت شبهات بأن الهجوم هو جزء من عمل واسع تقوم به دولة. وقد ألمح وزير الدفاع الأميركي ليئون بانيتا مؤخرا إلى أن الهجمات هي عمل إيراني. وقد كان موظف أميركي رفيع سابق أكثر وضوحا عندما قال: "إن الإدارة الأميركية تؤمن بأن إيران تقف وراء الهجوم في الخليج" .

يتضح من التحليل الذي أجراه خبير الحماية الأميركي جيفري كار عدة معطيات تربط إيران بالهجوم المذكور. فإيران هي الدولة الوحيدة التي يمكنها الوصول إلى الرمز الأصلي **Wiper** والذي اشتق منه على ما يبدو الفيروس **Shamoon**. يوجد لدى إيران حوافز كبيرة جدا لمهاجمة شركة النفط السعودية بسبب العقوبات الشديدة المفروضة على إيران في مجال الطاقة. كما فحصت شبهات حول علاقة حزب الله بالهجوم، وقد تم اعتقال عدد من موظفي شركة أرامكو والتحقيق معهم بهذا الخصوص.

مفاهيم بديهية:

يجب أن تثير مقدرة إيران على حرب التحكم الآلي قلق إسرائيل والولايات المتحدة ودول أخرى في الغـرب. وفي أعقاب الجرأة الشديدة التي بدت في محاولة اغتيال سفير السعودية في الولايات المتحدة، يقترح خـبراء أميركيـون عدم الاستخفاف بنوايا ومقدرة إيران وجرأتها على مهاجمة بنى حساسـة وحيويـة في الولايـات المتحـدة. وعـلى غـرار باقي العالم يمكننا الافتراض أن إيران التي تعرضـت هـي أيضـا لإحـدى هجـمات الـتحكم الآلي الأشـد ضراوة وتـدميرا، استقت جيدا العبر من الهجوم الذي تعرضت له من قبل الفيروس ستاكسنت، وهـي تـدرك القـوة التدميريـة الهائلـة الكامنة في تطوير وسائل هجوم تحكم آلي قادرة على إلحاق الأضرار بأجهزة الرقابة الصناعية.

إن تطـوير الإسـتراتيجية الإيرانيـة ومسـاقات بنـاء القـوة التـي تلتهـا تشـير إلى عمليـة تنظـيم منهجيـة كي تصـبح لاعبـا قويـا في مجـال حـرب الـتحكم الآلي. ويقـول الخـبراء أنـه طـرأ تقـدم دائـم عـلى مقـدرة الـتحكم الآلي ومقدرة المنفـذين الإيـرانيين. وقـد عقـب أحـدهم في أعقـاب الأنبـاء القائلـة أن مؤسسـات ماليـة أميركيـة تعرضـت لهجمات نسبت إلى إيران: "برنامج الـتحكم الآلي الإيـراني يشـبه برنامجهـا النـووي، فهـو لـيس ذكيـا بصـورة خاصـة، لكنـه يتقـدم سـنويا إلى الأمـام . لا يجـب الاسـتخفاف بالمقـدرة التكنولوجيـة الإيرانيـة، فـالبنى العلميـة في هـذه الدولة متطورة كما أن "احتيـاط رأس المـال الـبشري" واسـع. لـذا يمكننـا القـول أن إيـران سـتتمكن في غضـون فـترة قصيرة من أن تصبح عاملا أساسيا عـلى المسـتوى العـالمي في هـذا المجـال. إن هـذه التقـديرات تلقـى تأييـدا ودعـما مـن هجـوم الـتحكم الآلي الـذي تعرضـت لـه شركـة ارامكـو والتـي قـال في أعقابهـا جـيمس لـويس خبـير في مجـال الـتحكم الآلي: إن إيـران كانـت أسرع في تطـوير مقـدرتها الهجوميـة وأجـرأ عـلى صـعيد تفعيلهـا بصـورة لم نكـن نتوقعها. وبصورة عامة فإن العمليات التي تم اكتشافها ما هي سوى غيض من فيض للأعـمال الأخـرى التـي لا زالـت طي الكتمان. أضف إلى ذلك فإن تحسين المقدرة الدفاعية الإيرانية يتطلب من الجهات المهتمة بإعادة تنظـيم نفسـها للعمل في مجال شبكات منفصلة الواحدة عـن الأخـرى، أو حتـى ضـد شـبكة إيرانيـة خاصـة منفصـلة عـن الانترنـت.

ورغم أن التحدي القائم في بناء وفصل هذه الشبكة فصلا كليا هو عمل هائل جدا، إلا أن بالإمكان العثور على طرق للعمل في مثل هذا الوضع. إن نظرية الحماية المذكورة ستكون بمثابة تحد لا يستهان به أمام الجهات الراغبة في تنفيذ عمليات في مجال التحكم الآلي الإيراني.

ويمكننا أن نستخلص من خلال النشاطات التي نسبت إلى إيران والتي تطرقنا إليها أعلاه العديد من العبر. إن محاولة إيران الحصول على تصاريح SSL يشير إلى عملها في مواجهة مجموعات جماهيرية كبيرة، ومواجهة أهداف موضعية أقل، مثل الدول أو الشركات والمنظمات. ويبدو أن الأمر يتعلق بضرورة تشخيص ومراقبة جهات داخلية إيرانية، بيد أن العمل في هذا المجال يتيح الفرصة للقيام بعمليات في مواجهة أهداف أكثر موضعية مثل الدول والشركات.

وتجدر الإشارة إلى أنه وعلى الرغم من أن العمليات التي تم اكتشافها تشير إلى تنظيم ومنهجية في العمل، إلا أنه يبدو أن إيران لم تتجاوز الذروة التكنولوجية والتنظيمية التي يمكنها أن تحولها إلى جهة ذات كفاءة ودهاء كبيرين ، بيد أن الحوافز الإيرانية وعمليات بناء القوة والمقدرة التكنولوجية في الدولة سيتيح لها السير قدما بهذا الاتجاه بسرعة كبيرة.

إن الهجوم الذي تعرضت له شركة أرامكو يثير العديد من التساؤلات، التي يتعلق أولها بحقيقة أن الحماية الكلاسيكية من التهديدات عبر شبكة الانترنت غير كافية. وغالبية الخبراء يقبلون الافتراض القائل أن الشركة لم تول مسألة الحماية من الأخطار القادمة عبر الانترنت القدر الكافي من الجهد.

ومن الجدير بالذكر أن جهاز الحماية للشركة لم يتمكن من اكتشاف الفيروس الذي أدخل إليه عن طريق جهة داخلية في الشركة كانت تملك التصاريح الملائمة للدخول. ومن الجدير بالذكر أن منظومات الحماية القائمة والنموذجية لم تبن من أجل توفير الحماية ضد التهديدات الموضعية (APT)، والرموز الشيفرية "الشريرة" غير المعروفة (zero date) وغيرها، لذا ازدادت الضرورة للعمل على تطوير وسائل قادرة على توفير الحماية الأفضل في مواجهة التهديدات من هذا القبيل. ومن ضمن الاتجاهات الآخذة في التطور على هذا

الصعيد الاتجاه الرامي إلى تطوير وسائل تقوم على التشخيص، والحجب والتحييد للمسلكيات غير الطبيعية وغير المرغوبة في الحواسيب التي تتعرض للهجوم. وبمقدور مثل هذه الوسائل أن تحيّد التهديدات حتى في أعقاب نجاح الشيفرة "الشريرة" من التسلل للحاسوب الهدف.

أما الصورة الأخرى فتتعلق بالأهداف الهجومية الرامية بشكل رئيسي لتدمير معلومات بصورة شاملة ودون تمييز في عشرات آلاف الحواسيب في شركة النفط السعودية، على أن يتم أيضا جمع معلومات بصورة جزئية. وإذا كان بمقدورنا القول أن عمليات التحكم الآلي الاستخبارية مشروعة بصورة جزئية، فإن الهجوم واسع النطاق الذي شنته إيران على هدف مدني يشير إلى انتقالها إلى مرحلة الرد الانتقامية. ولا شك أن مثل هذا الانتقال يجب أن يقلق الجهات المسؤولة عن الحماية في الكثير من الدول. إن التصريحات التي أطلقها وزير الدفاع الأميركي ليئون بانيتا عن ضرورة محاسبة الجهات التي تقف وراء مثل هذا الهجوم، يؤكد ما قلناه حول القلق. لكن الفعل هو الذي سيحسم الأمور وليس مجرد القول.

ونظرا للأضرار المدمرة التي لحقت بإيران جراء الهجمات التي تعرضت لها عبر التحكم الآلي، يمكننا القول أنها تدرك جيدا حجم الاحتمالات الكامنة في هذا المجال، وستعمل على تطوير مقدرتها في المستقبل.

وعلى ضوء ذلك، فإن مسارات بناء القوة التي تطرقنا إليها آنفا، ستقود إيران في غضون فترة وجيزة كي تصبح لاعبا كبيرا في ساحات معارك التحكم الآلي لمهاجمة البنى الحيوية في الدول المعادية لها، و من ضمنها: الولايات المتحدة، وإسرائيل. مع خلق حالة فصل إلى أكبر حد ممكن في حالة اكتشاف تلك العمليات.

تستخدم إيران جماعات كبيرة من قراصنة الحاسوب المدنيين،مع محاولة خلق حالة فصل بينهم وبين النظام والمنظمات الإيرانية. وهذا الأسلوب يشابه الأسلوب المنتهج في العديد من دول العالم، مثل الصين وروسيا، وهو أسلوب يمكن الدول من التنصل من تحمل المسؤولية ونسب الاعتداءات لمدنيين، لذا ستكون هناك صعوبة بالغة في نسب اعتداءات التحكم الآلي لدولة إيران.

إن محور عمليات التحكم الآلي الإيرانية في إسرائيل والدول الغربية الأخرى، يتطلب العمل على إعادة النظر في عمليات التنظيم الدفاعية الموضعية، كما أن هناك حاجة إلى نظرية حديثة في كل ما يتعلق بالحماية في مجال التحكم الآلي. وإزاء التطور الواسع لإيران على هذا الصعيد، فإن إسرائيل تسعى لوضع مجال التحكم الآلي الإيراني على رأس أجندتها لجمع المعلومات الاستخبارية وعمليات الإحباط ، بصورة تمكنها من الاكتشاف المسبق للاستعدادات للقيام بعمليات هجوم وإحباطها قبل أن تبدأ.

وعلى غرار البرنامج النووي الإيراني، فإن التحدي لا يقتصر على دولة إسرائيل فقط ، بل أيضا على العديد من الدول الأخرى في الغرب، وأيضا دول الخليج. إن الهجوم الذي تعرضت له شركة أرامكو السعودية هو أكبر دليل على ذلك. لذا يجب العمل على طرح مبادرات تعاون على أوسع نطاق بين الدول في مجال العمل الاستخباري والإحباط والوقاية في مواجهة هجمات التحكم الآلي الإيرانية.

أضف إلى ذلك يجب على إسرائيل أن تواصل العمل على بناء رد دفاعي فعال، على أن يقوم على طبقات التحكم الآلي الثلاثة في الدولة:

الأولى: طبقة المنظمات الأمنية التي يجب عليها أن تدرس بصورة دائمة إمكانية التعرض لهجوم تحكم آلي إيراني والتأكد من أن الهجوم لم ينجح في العمل ولا بالمساس بالمناحي الحيوية للجهاز الأمني.

والطبقة الثانية: تتعلق بجهاز البنية التحتية الحيوية في الدولة التي تقوم بتوجيهها وإدارتها "سلطة حماية المعلومات " بناء على قرار الحكومة بهذا الصدد. والتحديات على هذا الصعيد تتطلب عمليات متواصلة وبشكل خاص في كل ما يتعلق بفهم صورة التهديد، والتعاون في مجال تبادل المعلومات بين الجهات المختلفة واستقاء العبر اللازمة من التهديد.

والطبقة الثالث: هي عدم الاستخفاف بالمقدرة الإيرانية في محاولتها المساس بالأعمال والصناعات التي لا تديرها أية جهات في الدولة. فالأعمال والصناعات في القطاع الخاص تعمل في غالبية الحالات من أجل حماية مخازن معلوماتها، ومن الصعب مطالبتها بحماية نفسها أمام احتمالات أن تتعرض لهجمات تحكم آلي من قبل

دولة أجنبية مثل إيران. لذا، فإن أهمية هيئة التحكم الآلي القومية الحاسمة تكمن في كونها الجهة الوحيـدة القـادرة على معرفة جميع أشكال الهجوم والتخطيط لكيفية مواجهتها والتصدي لها.

الفصل التاسع

نماذج لأشهر

هجمات "السايبر"

- OxOma هاجم آلاف بطاقات الائتمان الإسرائيلية مما ساهم في تناقص حركة المشتريات بالبطاقات بنسبة 10%.

- حصان طروادة فيروس إيراني نجح باختراق حواسيب تابعة لشخصيات إسرائيلية رفيعة.

- فيروس (فليم) يستخدم لغايات "التجسس الالكتروني" أي انه يمكن أن يسرق معلومات مهمة محفوظة في الحواسيب إلى جانب معلومات في أنظمة مستهدفة ووثائق محفوظة والمتصلين بالمستخدمين وحتى تسجيلات صوتية ومحادثات ثم يرسلها إلى خوادم في كافة أنحاء العالم.

- فيروس "ستاكسنت" هاجم ما لا يقل عن 30 ألف جهاز كمبيوتر في إيران دون التسبب في "أضرار خطيرة

- فيروس "لهب" ضرب في ايار 2012 شبكة الحواسيب والمعلومات الإيرانية في المنشآت التي تقوم إيران بتخصيب اليورانيوم فيها عبر آلاف أجهزة الطرد المركزي

---

* ضد إسرائيل:

- فيروس 'xOmar':

نشر الهاكر السعودي يوم 2012/1/6 على الانترنت المعلومات الخاصة بأحد عشر ألف بطاقة ائتمان إسرائيلية، نصفها على الأقل بطاقات عاملة. وقد أدى نشر هذه البطاقات إلى تناقص حركة المشتريات بالبطاقات بنسبة 10%.

وقال الهاكر-" قراصنة الكمبيوتر"- السعودي أن بحوزته معلومات عن حوالي مليون بطاقة ائتمان إسرائيلية، ونشر قائمة جديدة تضم معلومات حول أحد عشر ألفا، وقال أنه سينشر قريبا قائمة معلومات تتضمن ستين ألف بطاقة. بيد أن عملية الفحص التي أجرتها شركة "تو بي سكيور" الإسرائيلية ادعت أن أربعة آلاف بطاقة فقط من البطاقات التي نشرها هي بطاقات عاملة، وأن قسما منها نشر في القائمة السابقة.

وقال الهاكر " قراصنة الكمبيوتر" السعودي في مقابلة مع عدة وسائل إعلام إسرائيلية: إن هدفه يتمثل في المساس بإسرائيل.

وفحصت شركات الائتمان الإسرائيلية معلومات بطاقات الائتمان التي نشرها الهاكر" قراصنة الكمبيوتر" السعودي، ووجدوا أن غالبيتها تعود لشركة "يسرا كارد"، وقد اتضح أن هذه البطاقات تعود لزبائن ممن اعتادوا الشراء عبر الانترنت ببطاقات الائتمان.حيث اتصلت الشركات الإسرائيلية فورا بزبائنها الذين كشفت معلوماتهم وأوقفت بطاقات ائتمانهم. هذا ولم يتم اكتشاف أية خسائر لحقت بالزبائن، وقامت الشركات باستبدال بطاقات الائتمان بغيرها جديدة.

واتضح أن الهاكرز" قراصنة الكمبيوتر" العرب يتابعون مراكز الشراء المخصصة لليهود، فعلى سبيل المثال تمت سرقة المعلومات الخاصة بجميع الأشخاص الذين اشتروا منتجات وخدمات من أماكن مخصصة لليهود مثل المواد المتعلقة بالديانة اليهودية في إسرائيل والولايات المتحدة.

وادعى الخبير الإسرائيلي أمير بديده أن الهاكر" قراصنة الكمبيوتر" السعودي يسكن في المكسيك ويدعى عمر حبيب ويناهز التاسعة عشرة من العمر،وهو يدرس في كلية علوم الحاسوب في مركز للدراسات المتقدمة يدعى Hidalguense Cenhies وأنه من دولة الإمارات العربية.

وأضاف بديدة أن الهاكر" قراصنة الكمبيوتر" ارتكب العديد من الأخطاء خلال اقتحامه للمواقع الإسرائيلية، وأكبر تلك الأخطاء اتصاله بوسائل الإعلام الإسرائيلية، حيث تمكنت خلال بضع ساعات من الوصول إليه، وتحديد مكانه وجمع معلومات عنه، وأنه يأمل أن تؤدي المعلومات التي جمعها من إلقاء القبض عليه وتسليمه إلى إسرائيل لمحاكمته.

ورد OxOma وهو الاسم الذي استخدمه الهاكر" قراصنة الكمبيوتر" السعودي: هذا يعبر عن فشل إسرائيلي جديد، لو كنت أنا الشخص الذي حدده لكنت الآن في السجن". وقال عمر حبيب خلال مكالمة مع موقع يديعوت " لن تنجحوا في معرفة مكاني وسأواصل اختراق مواقعكم".

وأضاف عمر قائلا أنا هاكرز " قراصنة الكمبيوتر" متطور اعرف كل شيء عن الانترنت وأنا اعرف كيف أموّه على نفسي والصورة التي نشرتها "إسرائيل" للشخص عمر السعودي هي صورة لشخص بريء ليس لها علاقة بي إطلاقا. وقال: "أتحدى كل العالم بأن يجد مكاني فاللعبة قد بدأت".

وأضاف عمر: "أنا أتحدى "إسرائيل" وبعد أسبوعين سأنشر معلومات جديدة مخترقة انتم الخاسرون وأنا الكاسب فاللعبة في بدايتها وانتم الخاسرين".

وسخر عمر خلال المحادثة مع يديعوت من محاولات المخابرات الإسرائيلية للعثور عليه قائلا " إن نجح الطالب الإسرائيلي الغبي بالعثور علي خلال 8 ساعات عمل متواصلة فماذا كان سيفعل الموساد فأنا لا زلت هنا ولا احد يستطيع العثور علي تأكدوا من ذلك".

وقال لدي معلومات خاصة بمليون إسرائيلي، مهدداً بمواصلة نشر تلك المعلومات، حيث قال: "سأواصل الاختراقات وليأخذ الموساد والانتربول أي وقت يحتاجونه لإيجادي هل يكفيهم أسبوعين ؟

وعندما سئل هل هو نادم على ما يفعله قال :"لا بل سأواصل اختراق الشركات الإسرائيلية التالية (شركات البناء والمقاولات التي تعمل لصالح الجيش الإسرائيلي، وسأخترق منظومة SCADA (منظومة تستخدم للإشراف والسيطرة وجمع المعلومات)" .

وفي صباح 2012/1/16 تعطل موقعا الانترنت التابعان لشركة الطيران الوطنية العال ولبورصة تل ابيب . وكان قرصان الحواسيب السعودي قد حذر من نية عدد من رفاقه مهاجمة هذين الموقعين.

الهاكرز السعودي لا يكتفي باختراقه لمواقع إسرائيل الرئيسية فهو أيضا يسخر من إسرائيل والإسرائيليين وخاصة من نائب وزير الخارجية الإسرائيلي داني ايلون الذي هدد الهاكرز السعودي (اوكس عمر بالقتل) فقد طالب عمر من أيلون أن يعتذر عن كل كلمة قالها ضده.

وقد أرسل الهاكرز عمر لموقع يديعوت عبر البريد الالكتروني رسالة قال فيها بأنه انضم لقائمة هاكرز عرب يحملون اسم Nightmare حيث يعمل الهاكرز العرب عبر قناة خاصة بهم قادرة على الإطاحة بكل موقع إسرائيلي على شبكة الانترنت .

- حصان طروادة :

أعلن مختبر "كسبسكي سكيليرت " الإسرائيلي المتخصص بحماية المعلومات الالكترونية يوم 2012/7/18" اكتشافه "حصان طروادة " إيراني نجح باختراق حواسيب تابعة لشخصيات إسرائيلية رفيعة.

وقال المختبر أن " الحصان الإيراني " الذي يحمل اسم " مهادي" يعمل ضد الحواسيب الإسرائيلية وحواسيب شرق أوسطية أخرى منذ عدة أشهر ويعمل وفقا لشركة الحماية على جمع معلومات وصور ومعلومات خطيرة وحساسة تتعلق بشخصيات إسرائيلية ذات علاقة وثيقة بمشاريع البنية التحتية إضافة لمعلومات تتعلق بجهات وأوساط مالية ومؤسسات أكاديمية ويقوم الفيروس بنقل المعلومات فورا لزارعيه .

واكتشف المختبر داخل الفيروس مكونات خاصة باللغة الفارسية وأخرى بالتاريخ الفارسي ما يشير إلى إيران كمصدر للفيروس.

وادعى خبراء شركة الحماية بـأنهم لاحظـوا 800 حاسـوب إيـراني جـرى اختراقهـا عـبر هـذا الفـيروس و 54 حاسوبا إسرائيليا وحواسيب أخرى في دول مختلفة وذلك في فترة الثمانية أشهر الماضية.

وأظهرت عملية "التشريح" التي خضعت لها الحواسيب الإسرائيلية التي كانت ضحية الفـيروس أن زارعـي الفيروس اخترقوا حواسيب رجال أعمال إسرائيليين على علاقة بمشاريع البنية التحتية الوطنيـة بمـا في ذلـك المؤسسـات الاقتصادية الإسرائيلية إضافة لحواسيب طلبة هندسة وأخرى تعود لجهات حكومية في عدد من دول الشرق الأوسـط .

- هجمة "OpIsrael"

أصاب هجوم التحكم الآلي ضد إسرائيل يوم 2013/4/6 -وإن يكن حجمه صغيرا نسبيا- مئات المواقع، رغم أن أية مواقع هامة لم تصب فعليا. وقد قامت غالبية المواقع بمنع دخول المستخدمين من خارج إسرائيل.

وبدأ هجوم التحكم الآلي الـذي خطـط لـه ضـد إسرائيـل يـوم 2013/4/6 ولـيس 2013/4/7 – كـما كـان مقررا- وقد تم اختراق مئات الحواسيب. وقال رئيس الهيئة الإسرائيلية لحماية المعلومات آفي فيسمان: أنه تم اخـتراق أكثر من سبعمائة حساب لمستخدمي فيسبوك، وإن المواقع التي تم اختراقهـا عديمـة القيمـة، ولـيس مـن المتوقـع أن تكون هناك إصابة خطيرة لبنية الانترنت في إسرائيل. ويقول: "يجب على كل مواطن أن يتخذ الاحتياطات اللازمة لمنع اختراق موقعه، وأن لا يحتفظ على الحاسوب الشخصي بمعلومات شخصية، ولا بطاقات ائتمان، ولا أرقام سرية، وعدم الرد على أية رسالة تصل على البريد الإلكتروني إذا لم نكـن نعرفهـا، وأن نكـون حـذرين تجـاه أيـة معلومـات نتلقاهـا وكيفية استخدامها".

وكان من المزمع انطلاق العملية يوم الأحد، السابع مـن أبريـل2013، إلا أن الهجـمات الإلكترونيـة بـدأت مبكراً منذ عصر السبت، حيث اخترقت مواقع حكومية إسرائيلية ومواقع بارزة لجامعات ومؤسسات بنكيـة وتجاريـة هناك، بالإضافة إلى الآلاف من الصفحات الإسرائيلية على شبكات التواصل الاجتماعي.

وتضمنت العملية اختراق وإيقاف مواقع بارزة مثل موقع مجلس الوزراء الإسرائيلي، gov.il، ومواقع وزارة الجيش الإسرائيلي والتعليم والاستخبارات وسوق الأوراق المالية والمحاكم الإسرائيلية وشرطة تل أبيب وحزب كاديما وبنك القدس.

وقالت صحيفة هآرتس الإسرائيلية أن نحو 19 ألف حساب إسرائيلي على مواقع التواصل الاجتماعي تم اختراقه، وذلك في اليوم الذي كانت تستعد فيه "إسرائيل" لإحياء ذكرى المحرقة المزعومة.

ووضع القراصنة رسائل مختلفة داعمة للأسرى والقضية الفلسطينية، وأخرى مندددة بالسياسة الإسرائيلية تجاه الفلسطينيين على المواقع المخترقة، إلا أن أغلب تلك المواقع أغلقت تماماً وذلك لحين التعامل مع الاختراق وإعادتها مرة أخرى.

ووصف التلفزيون الإسرائيلي عبر قناته الثانية الهجمة الإلكترونية بأنها حرب تشن على "إسرائيل"، كما وصفت وسائل إخبارية محلية إسرائيلية الهجمة الإلكترونية بأنها الأكبر من نوعها.

وأوضح القراصنة القائمون على العملية عبر حسابهم الرسمي على موقع تويتر استمرار هجومهم الإلكتروني ضد المواقع الإسرائيلية وبعض الحسابات لناشطين داعمين للسياسة الإسرائيلية تجاه الشعب الفلسطيني، حيث يأملون أن تصل أصوات الفلسطينيين إلى العالم عبر تلك الهجمات.

وأعلنت 'أنونيموس' أن المجموعات التي قامت بالهجوم هي 'سكتور 404' (القطاع 404)، و'أنونيموس' و'ريد هاك'، حيث قامت مجموعة 'سكتور 14' بنشر ما أسمته 'إنكاراً لتعرض الخدمة للهجوم' في حين قامت 'أنونيموس' و'ريد هاك' باختراق موقع الموساد، لتتمكن من تسريب معلومات بالغة السرية والحساسية عبر تويتر و'غوغل دوكس' (وثائق Google).

وتضمنت القوائم المسربة بطاقات هوية وعناوين بريد إلكتروني وأرقام مناطق بريدية، وأرقام هواتف المدن والولايات (الأمريكية) التي يعيش أو ينشط فيها عملاء الموساد،وقالت 'أنونيموس' أنه بما أن المعلومات قد

سربت فإنه من الصعب الاحتفاظ بها إلكترونياً، إذ أن السلطات قامت بإلغائها وإن كانت ما زالت متوافرة على روابط قامت 'أنونيموس' بنشرها بما في ذلك عبر 'غوغل دوكس'.

***ضد إيران :**

- فيروس فليم :

أعلنت شركة روسية لإنتاج البرامج المضادة للفيروسات المعلوماتية أنها اكتشفت فيروسا جديدا يتمتع بقوة تدميرية لا سابق لها تستهدف إيران بشكل رئيسي ويمكن استخدامه "سلاحا الكترونيا" من قبل الغرب وإسرائيل.

وقالت "كاسبيرسكي لاب" -التي تعد من اكبر شركات إنتاج البرامج المضادة للفيروسات في العالم، في بيان في ساعة متأخرة مساء 2012/5/28 -إن خبراءها اكتشفوا الفيروس المعروف باسم فليم (الشعلة) خلال تحقيق أجراه الاتحاد الدولي للاتصالات.

ويبدو أن إيران هي الجهة الرئيسية التي يستهدفها الفيروس إذ يأتي الإعلان بعد شهر فقط على تأكيد إيران أنها أوقفت انتشار فيروس يمحو البيانات استهدف خوادم أجهزة الكمبيوتر في قطاعها النفطي.

وقالت الشركة إن الفيروس الجديد "يتمتع بقوة تزيد على عشرين مرة عن ستاكسنت" الذي رصد في 2010 واستخدم ضد البرنامج النووي الإيراني.

وأضافت كاسبيرسكي أن الفيروس فليم يستخدم لغايات "التجسس الالكتروني" أي انه يمكن أن يسرق معلومات مهمة محفوظة في الحواسيب إلى جانب معلومات في أنظمة مستهدفة ووثائق محفوظة والمتصلين بالمستخدمين وحتى تسجيلات صوتية ومحادثات ثم يرسلها إلى خوادم في كافة أنحاء العالم.

وقالت إن الفيروس فليم "يستخدم بفاعلية كسلاح الكتروني لمهاجمة كيانات في دول عدة". وتابعت إن "مستوى تعقيد وعملانية البرنامج الذي رصد مؤخرا يتجاوز كل التهديدات المعلوماتية المعروفة حتى الآن."

ولم يتم الكشف عن مصدر الفيروس "ستاكسنت" لكن الشكوك حامت حول الولايات المتحدة وإسرائيل اللتين تتهمان إيران بالسعي لصنع سلاح ذري.

وقال الكسندر غوستيف كبير خبراء الأمن في "كاسبيرسكي لاب" أن إيران هي الدولة الأكثر تضررا بالفيروس فليم تليها إسرائيل والأراضي الفلسطينية والسودان وسوريا ولبنان.

وأوضح في مقال تحليلي أن "جغرافية تلك الأهداف ومستوى تعقيد الفيروس لا يدع مجالا للشك في أن الأبحاث التي أجريت عليه جرت برعاية دولة."وقال انه من الواضح أن هدف الفيروس "جمع المعلومات" عن عمليات دول في الشرق الأوسط مثل إيران ولبنان وسوريا. غير أن "مصدره مجهول" مثل "ستاكسنت" والفيروس السابق "دوكو". وأضاف أن "فليم" غير مصمم لسرقة الأموال من حسابات مصرفية. وهو أيضا يختلف عن أدوات تخريب بسيطة يستخدمها قراصنة المعلوماتية."

وسارعت إيران يوم 2012/5/29 إلى التأكيد بأنها تمكنت من إنتاج فيروس مضاد قادر على كشف وتدمير الفيروس المعلوماتي الجديد.

وبحسب بيان نشر على موقع مركز التنسيق الإيراني لمكافحة الهجمات المعلوماتية فان مركز ماهر التابع لوزارة الاتصالات الإيرانية "تمكن من كشف الفيروس "فليم" ثم تحضير فيروس مضاد قادر على التعرف عليه وتدميره." وأضاف البيان أن هذا الفيروس المضاد "في تصرف أجهزة وإدارات طلبته" لكن دون تحديد تاريخ أو كيفية اكتشاف الفيروس ولا الأضرار التي قد يكون أحدثها في إيران.

وأوضحت "كاسبيرسكي لاب" أن "المعلومات الأولية تشير إلى أن هذا البرنامج المؤذي موجود منذ أكثر من سنتين في الأنظمة، منذ آذار 2010."

ويقول خبراء في الشركة انه احد البرامج الأكثر تقدما، وقال خبراء الشركة إن هذا هو الهجوم الأكثر تعقيدا حتى الآن. ووفقا لهؤلاء الخبراء فقد ضرب الفيروس 189 حاسوبا في إيران و 98 حاسوبا في مناطق السلطة الفلسطينية و 32 حاسوبا في السودان و 30 حاسوبا في سوريا و 18 في لبنان و 10 في

السعودية وحواسيب في مصر . وتضفي حقيقة ضربه فقط لحواسيب في دول عربية وإسلامية تساؤلات كثيرة حول مصدره.

كما قال الفريق الوطني للاستجابة لطوارئ الكمبيوتر في إيران إن فيروس "فليم" قد يكون مرتبطا بهجمات على الإنترنت في الآونة الأخيرة قال مسؤولون في طهران إنها مسؤولة عن فقدان كم هائل من البيانات في بعض أنظمة الكمبيوتر الإيرانية.

وبحسب لوران هسلو المسؤول عن الأمن في شركه "سيمانتك" التي تصنع برنامج "نورتون" لحماية أجهزة الكمبيوتر، فان "فليم" قد يكون استخدم لشن هجمات على "أهداف بالغة الأهمية" وقال "يمكن تحديد عدد أجهزة الكمبيوتر المستهدفة بالعشرات أو ربما بالمئات لا أكثر"، مضيفا" واضح انه نظرا لمستوى التعقيد فيه فان الجهة الداعمة له ذات نفوذ."وأوضح "هل هي دولة؟ جيش؟ قوات شبه عسكرية؟ من الصعب تحديد ذلك."

- دودة ستاكسنت:

تسلل فيروس "ستاكسنت"، الذي يهاجم البرامج المعلوماتية لإدارة الصناعة، إلى ما لا يقل عن 30 ألف جهاز كمبيوتر في إيران دون التسبب في "أضرار خطيرة"، حسب مسؤولين إيرانيين نقلت أقوالهم 26-9-2010، صحف إيرانية تحدثت عن "حرب معلوماتية."

ونقلت صحيفة "إيران دايلي" الحكومية عن محمود ليايي مسؤول التكنولوجيا المعلوماتية في وزارة الصناعة، أنه تم إحصاء 30 ألف عنوان آي بي لهويات أجهزة كمبيوتر تعرضت لفيروس "ستاكسنت" حتى الآن في إيران.

ويبحث فيروس "ستاكسنت" الذي اكتشف في 2010 ، في أجهزة الكمبيوتر التي يتسلل إليها، عن برنامج خاص طورته شركة سيمنز الألمانية ويتحكم بأنابيب النفط والمنصات النفطية في البحر ومحطات توليد الكهرباء وغيرها من المنشآت الصناعية.

وبحسب صحيفة "فايننشال تايمز" التي كشفت القضية، فإنه أول فيروس معلوماتي لا يكتفـي بشـل نظـام معلوماتي، بل يهدف إلى تدمير المنشآت فعلياً. ويبـدو أن "ستاكسـنت" هـاجم بشـكل خـاص إيـران، وكـذلك الهنـد وإندونيسيا وباكستان.

وأعلن ليايي أن "ستاكسنت ينقل إلى جهة معينة معلومات عن خطوط الإنتاج الصناعي والأنظمة الآليـة. ثم يعكف مصممو الفيروس على معالجة المعلومات لتدبير مؤامرات ضد البلاد". وأضـاف أن "حكومـة أجنبيـة تقـف على الأرجح وراء هذا الفيروس" نظراً إلى درجة تعقيده، من دون إضافة مزيد من التوضيحات.

وتحدثت "إيران دايلي" عن "حرب معلوماتية يشنها الغرب على إيران"، مستندة إلى عـدة خـبراء يتهمـون الولايات المتحدة وإسرائيل.

وأضاف ليايي أن الصناعات الإيرانية بصدد تلقي أنظمة تهدف إلى مكافحة "ستاكسنت"، مؤكداً أن إيـران قررت عدم استخدام الفيروس المعادي الذي أعدته سيمنز "لأنه قد يكون يحمل صيغة جديدة من الفيروس."

من جانبه أكد وزير الاتصـالات وتكنولوجيـات الإعـلام رضـا تقـي بـور انـه "لم يشر إلى أي أضرار كبـيرة في الأنظمة الصناعية في البلاد" بسبب "ستاكسنت" كما أضافت "إيران دايلي". وتابع أن "الفيروس لم يستطع التسلل إلى الجهاز الحكومي أو إلحاق أضرار كبيرة به."

وعلى الصعيد الميداني، أعلن مدير شركة تكنولوجيات الإعلام التابعة لوزارة الاتصال سيد مهديون أن "فرق اختصاصيين بدأت تقضي منهجياً على الفيروس." ولم يتحدث أي مسؤول عن احتمال تضرر منشآت نووية إيرانية مـن الفيروس.

وأفادت "فايننشال تايمز" أن أول محطة نووية إيرانيـة في "بوشـهر" قـد تكـون أصـيبت بـالفيروس، بيـنما أكدت سيمنز أنها لم تسلم البرنامج المعني بانتشار الفيروس إلى تلك المحطة النووية التـي بنتهـا، روسـيا التـي سـتبدأ العمل بحلول نهاية السنة.

وستاكسنت: هو فيروس هاجم أنظمة المعلومات في إيران صنع خصيصا للإضرار بأجهزة الطرد المركزي لتخصيب اليورانيوم في المنشآت النووية الإيرانية ، وكان يستهدف -على ما يبدو -البرنامج النووي الإيراني، وذلك استنادا إلى تحليل شفرة الفيروس.

ويعتقد الخبراء الأمريكيون أن الفيروس "ستاكسنت" صنع على الأرجح خارج الولايات المتحدة. وأثبت الخبراء بعد إجراء تحليل جديد لأهداف ونمط عمل الفيروس انه كان يسبب عطلا في محركات تابعة لأجهزة الطرد المركزي عن طريق إثارة تغيرات حادة في سرعة دوران هذه الأجهزة.

ويعتقد الخبراء النوويون انه كان يمكن أن تسبب هذه الهجمات في توقف المئات من أجهزة الطرد المركزي في مصانع تخصيب اليورانيوم في إيران، علما أن مراقبين من الوكالة الدولية للطاقة الذرية كانوا قد أكدوا أن إيران اضطرت منذ صيف عام 2009 إلى تبديل المئات من تلك الأجهزة بعد تعطيلها عن العمل.

و هاجم الفيروس أيضا الهند واندونيسيا وعدد من البلدان عام 2010.و يعمل هذا الفيروس بالأخص على أنظمة شركة سيمينس.

- فيروس "اللهب":

قامت الولايات المتحدة و"إسرائيل" سوية بتطوير فيروس الحاسوب "لهب" الذي ضرب في أيار 2012 شبكة الحواسيب والمعلومات الإيرانية في المنشآت التي تقوم إيران بتخصيب اليورانيوم فيها عبر آلاف أجهزة الطرد المركزي، مشيرة إلى أن هذا الفيروس قام بعد إدخاله باختراق شبكة المعلومات الإيرانية ونسخها وتحويلها للجهة التي قامت بتطويره، سعيا إلى وقف المشروع الإيراني وشله عن العمل.

وقالت صحيفة "واشنطن بوست": "إن التقرير يستند إلى معلومات وإفادات من مسؤولين رفيعي المستوى شاركوا في تطوير ذلك الفيروس، والذي تم تطويره بحسب الصحيفة بالتعاون بين وكالة المخابرات المركزية الأمريكية "السي أي إيه" ووكالة الأمن القومي الأمريكية من جهة وبين الجيش الإسرائيلي من جهة

ثانية بهدف جمع المعلومات الاستخبارية عبر متابعة البريد الالكتروني والمضامين الواردة عبره والرسائل المتبادلة.

وأشار أحد المسؤولين في حديثه مع صحيفة "واشنطن بوست" إلى أن فيروس "اللـهب" والفيروس السـابق المعروف باسم "دودة ستاكسنت" هما جزء من خطة أوسع وأشمل يتم تطبيقها في الأشهر الأخيرة.

*ضد دول الخليج:

- فيروس"شامون":

هجوم التحكم الآلي الذي شن على حواسيب شركة الـنفط السـعودية وحواسـيب شركـة الغـاز في الإمـارات الخليجية، بدأ يتضح بصورة تدريجية، كأذكى وأخطر هجوم يتم شـنه عـلى الخلـيج حتـى الآن. ويشـك خـبراء حمايـة غربيون أن هذا الهجوم – الذي تبنته مجموعتان إسلاميتان- تقف خلفه دولة، ويقول بعض هؤلاء الخـبراء إن إيـران هي التي تقف وراء الهجوم.

وجرى الهجوم في الخامس عشر من آب2012 على حواسيب شركة النفط السعودية الوطنية "أرامكو"، وقد أفادت مصادر الشركة أن ثلاثين ألف موقع عمل – حواسيب- تضررت، إضافة إلى ألفي مستخدم. وأفادت الأنباء بعـد ذلك عن هجوم على حواسيب شركة الغاز القطرية "راسجاز" وكذلك شركة الغاز الإماراتية. لكن الهجوم لم يتمكن من إلحاق أية أضرار بعملية ضخ الغاز أو النفط. وقد قامت شركة أرامكو بوقف جميع إمكانيات الدخول إلى منظومـات حواسيبها من الخارج على أمل أن تتمكن من إصلاح الضرر، كما اجريت عمليات إصلاح حواسيب الشركة القطرية.

ويتعلـق الأمـر بفـيروس شـبيه للفـيروس الـذي هـاجم شركـات الطاقـة في الخلـيج. وقـد أخـذت ثـلاث مجموعات من قراصنة الحاسوب عـلى عاتقهـا مسـؤولية الهجـوم، وأرفقـت المجموعـة المسـماة "مجموعـة الشـبيبة العربية" مع بيان تحمل المسـؤولية شـتائم للعائلـة السـعودية الحاكمـة. بيـد أن قـوة الهجـوم تشـير إلى أن الجهـات التي تقف خلفه أكبر بكثير من مجموعات صـغيرة غـير معروفـة. ويشـبه الفـيروس الـذي هـاجم السـعودية والـذي

أعطته شركة الحماية "كاسبرسكي" اسم "شامون" الفيروس "وييفر" الذي هاجم حواسيب وزارة النفط الإيرانية قبل بضعة أشهر. ولا شك أن بمقدور إيران أن تنسخ هذا الفيروس وتستخدمه ضد أعدائها.

- قرصنة إسرائيلية**IDF-TEAM** ":

- أعلن قراصنة الحاسوب الإسرائيليون2012/1/17 أنهم ردوا على الهجوم السعودي "عمر" وخربوا موقع بورصة الأوراق المالية في السعودية وأبو ظبي. ويبدو أن الأضرار التي ألحقوها بالموقع لم تكن كبيرة، واقتصرت على منع دخول الموقع على من يريد الدخول إليه عبر إغراق الموقع بطلبات الدخول.

المجموعة التي تطلق على نفسها "IDF-TEAM" -فريق الجيش الإسرائيلي- استطاعت أن تقتحم موقع البورصة المركزي في العاصمة السعودية الرياض وتعطيله بشكل كامل، وذلك رداً على اقتحام الموقع الالكتروني لشركة الطيران الإسرائيلية "العال" وموقع البورصة الإسرائيلية، وموقع بنك "ليؤمي" مما أدى إلى تعطيل تلك المواقع بشكل كامل.

وقالت المجموعة:" في ردنا الأولي على الهجوم السعودي على المواقع الإسرائيلية نعلن أن موقع البورصة السعودية لم يعد متوفراً في هذه اللحظات، وهذه هي مجرد البداية فقط، وفي حال استمرار الهجمات على المواقع الإسرائيلية فإن موقع نظام الإدارة السعودي سيخترق.

- مجموعة القراصنة الإسرائيليين المسماة "الذرة" نشرت 2012/1/19 (4800) بطاقة ائتمان لمواطنين من الدول العربية، بما فيها الأرقام السرية والرموز وأرقام الحماية ونوع الباقة وتاريخ صلاحيتها. وقالوا: إنهم حصلوا على هذه المعلومات جراء اختراقهم لأحد البنوك السعودية الكبيرة. وقالت هذه المجموعة أنها تعمل على مساعدة القرصان الإسرائيلي المسمى حنيبعل لقطر والذي قام بنشر آلاف العناوين الالكترونية وحسابات فيسبوك لمواطنين عرب، وقد كتب في موقع النشر: "ستكون هذه الحرب طويلة، لكننا سننتصر، إن هذه الحرب لم تنته مع قراصنة الحاسوب العرب".

***ضد أميركا:**

- شنت إيران أيلول 2012 سلسلة من الهجمات الإلكترونية المعطلة ضد عدد من المصارف والشركات الأميركية الكبرى، في حركة انتقامية واضحة ردا على ما تفرضه الدول الغربية عليها من عقوبات اقتصادية بغية عرقلة تقدمها في برنامجها النووي، بحسب مسؤولين أميركيين في الاستخبارات وفي دوائر أخرى.

واستهدفت الهجمات المواقع الإلكترونية لمصرف «جي بي مورغان تشيز» و«بنك أوف أميركا»، ونفذتها إيران، على حد قول جوزيف ليبرمان، رئيس لجنة الأمن الداخلي والشؤون الحكومية، يوم الجمعة.

وشك مسؤولون أميركيون في ضلوع إيران في هجمات إلكترونية سابقة على مؤسسات أميركية وأوروبية هنا وفي الشرق الأوسط، يعود بعضها إلى شهر (كانون الأول). وذكر موقع «واشنطن فري بيكون» الإلكتروني التابع لتيار المحافظين، قول الذراع الاستخباراتية لهيئة الأركان المشتركة، في تحليل بتاريخ 14 سبتمبر 2012، إن الهجمات الإلكترونية التي تستهدف المؤسسات المالية جزء من حرب سرية إيرانية أكبر.

وعلى عكس الهجمات الإلكترونية التي عطلت منشآت تخصيب اليورانيوم الإيرانية عن العمل والتي تنسب إلى الولايات المتحدة وإسرائيل، يرى الخبراء أن الهجمات التي تشنها إيران تستهدف تعطيل المواقع الإلكترونية التجارية.

- في يوم 2011/12/4 أعلن الإيرانيون أن بحوزتهم الطائرة الشبح الأمريكية الأكثر سرية، والتي تعمل دون طيار - من طراز RQ-170 وأنه عدا الضرر البسيط الذي لحق بها، فإن جميع النظم الإلكترونية السرية بحالة جيدة، أي أنها تعمل .

وفي يوم الاثنين 2011/12/5 أعترف متحدث عسكري أمريكي أن الطائرة حقا بحوزة الإيرانيين، وأنه من الواضح أن الطائرة بالفعل لم تتعرض للإسقاط بنيران إيرانية. بمعنى آخر، نجح الإيرانيون في السيطرة عن بعد في النظم الإلكترونية للطائرة – الشبح الأمريكية، وأنزلوها على الأراضي الإيرانية .

والوصف الإيراني الذي قال أن الشبح تضررت بشكل طفيف، يعني أن الطائرة السرية تضررت في جناحيها خلال هبوطها، بسبب عدم خبرة طاقم الحرب الإلكترونية والإستخباراتية الإيراني في إنزال طائرات من هذا النوع.

تم بحمد الله

الكتب الصادرة عن دار الجليل

تسلسل	العنوان	المؤلف او المترجم
1.	عمود النار "الأسطورة التي قامت عليها إسرائيل"	ترجمة : غازي السعدي
2.	الاستيطان "التطبيق العملي للصهيونية"	عبد الرحمن أبو عرفة
3.	حرب الجليل (نافذ)	بدر عبد الحق وغازي السعدي
4.	الكتاب السنوي "1981"	غازي السعدي ونواف الزرو وغسان كمال
5.	الكتاب السنوي "1982"	غازي السعدي ونواف الزرو وغسان كمال
6.	الحرب الفلسطينية الإسرائيلية في لبنان (1) شهادات ميدانية	غازي السعدي وبدر عبد الحق
7.	الحرب الفلسطينية الإسرائيلية في لبنان (2) معركة بيروت	مايكل جانسن - ترجمة : محمود برهوم
8.	الحرب الفلسطينية الإسرائيلية في لبنان (3) وثيقة جرم وإدانة	غازي السعدي
9.	الحرب الفلسطينية الإسرائيلية في لبنان (4) أهداف لم تتحقق	غازي السعدي
10.	الحرب الفلسطينية الإسرائيلية في لبنان (5) معتقل أنصار وصراع الإرادات (نافذ)	سليم الجنيدي
11.	الحرب الفلسطينية الإسرائيلية في لبنان (6) الحرب المضللة	زئيف شيف وايهود يعاري - ترجمة : غازي السعدي
12.	الحرب الفلسطينية الإسرائيلية في لبنان (7) فظائع الحرب اللبنانية	دوف يرميا - ترجمة : زكي درويش
13.	الحرب الفلسطينية الإسرائيلية في لبنان (8) هزيمة المنتصرين وانتصار القضية	إعداد : اللجنة ضد الحرب في لبنان
14.	الحرب الفلسطينية الإسرائيلية في لبنان (9) الأسرى اليهود وصفقات المبادلة	غازي السعدي
15.	رسائل من قبل الحصار	أبو عمار
16.	يوميات من سجون الاحتلال "زنزانة رقم 7"	فاضل يونس
17.	المثلث الإيراني: العلاقات السرية الإسرائيلية الإيرانية الأمريكية "الكتاب الأول"	شموئيل سيغف - ترجمة: دار الجليل
18.	المثلث الإيراني: العلاقات السرية الإسرائيلية الإيرانية الأمريكية "الكتاب الثاني"	شموئيل سيغف - ترجمة : دار الجليل

.19	هل يوجد حل للقضية الفلسطينية؟ "مواقف إسرائيلية"	ألوف هوروبين - ترجمة : غازي السعدي
.20	عملية الدبويا كما يرويها منفذوها	درويش ناصر – محامي الدفاع
.21	مراكز القوى ونموذج صنع القرار السياسي في إسرائيل (نافذ)	د. نظام بركات
.22	مشاريع التسوية للقضية الفلسطينية	منير الهور وطارق الموسى
.23	غوش أيمونيم – الوجه الحقيقي للصهيونية	داني روبنشتاين ترجمة : غازي السعدي
.24	رؤى مستقبلية عربية في الثمانينات	د. أحمد صدقي الدجاني
.25	أيام دامية في المسجد الأقصى	د. أحمد العلمي
.26	حق الشعب الفلسطيني في تقرير المصير	يوسف محمد القراعين
.27	الأحد الأسود	توماس هارس – ترجمة: حسن مشعل
.28	برتوكولات حكماء صهيون (المجلد الأول)	عجاج نويهض
.29	برتوكولات حكماء صهيون (المجلد الثاني)	عجاج نويهض
.30	الأردن وفلسطين	د. سعيد التل
.31	الاقتصاد الإسرائيلي بين دوافع الحرب والسلام	د. فؤاد بسيسو
.32	الاستعمار وفلسطين	رفيق شاكر النتشة
.33	الحرب من أجل السلام	عيزر وايزمن - ترجمة : غازي السعدي
.34	الموساد "جهاز المخابرات الإسرائيلية"	دنيس ايزنبرغ - ايلي لاندو - واوري دان
.35	التوازن العسكري في الشرق الأوسط	إعداد مركز الأبحاث الاستراتيجي التابع لجامعة تل أبيب
.36	الكتاب الأسود عن يوم الأرض 30 آذار 1976	إصدار اللجنة القطرية للدفاع عن الأراضي العربية في فلسطين المحتلة
.37	في سربية الصحراء	الشاعر سميح القاسم
.38	الخيار النووي الإسرائيلي	شاي فيلدمان - ترجمة : غازي السعدي
.39	انتهاك حقوق الإنسان في الأراضي المحتلة	إعداد منظمة القانون في خدمة الانسان ترجمة سليم أبو غوش
.40	نقاط فوق الحروف	خالد الحسن
.41	قراءة سياسية في مبادرة ريغان	خالد الحسن
.42	فلسطينيات	خالد الحسن
.43	الاتفاق الأردني الفلسطيني	خالد الحسن
.44	من ملفات الإرهاب الصهيوني في فلسطين (1) جرائم الأرغون وليحي	تأليف : يعقوب إلياب - ترجمة : غازي السعدي
.45	من ملفات الإرهاب الصهيوني في فلسطين (2) مجازر وممارسات	غازي السعدي
.46	من ملفات الإرهاب الصهيوني في فلسطين (3) دور الهاغناة في إنشاء إسرائيل	د. حمدان بدر

47. فلسطين تأريخا ونضالا — نجيب الأحمد
48. فلسطينيات في سجن النساء "طيور نفي ترتسا" — المحامي وليد الفاهوم
49. شوكة في عيونكم — مائير كهانا - ترجمة غازي السعدي
50. اتفاقيات السلم المصرية – الإسرائيلية — محمد الرفاعي
51. الجذور "وثيقة الأوقاف الإسلامية" — فتحي فوراني
52. فلسطين الأرض والوطن "قرية الدوايمة" — موسى عبد السلام هديب
53. خط الدفاع في الضفة الغربية — آرييه شليف - ترجمة : غازي السعدي
54. تشريقة بني مازن — د. عبد اللطيف عقل
55. القمع والتنكيل في سجن الفارعة — إعداد : لجنة الحقوقيين الدولية
56. صورة العربي في الأدب اليهودي — د. رايز دومب - ترجمة : عارف عطاري
57. الشخصية العربية في الأدب العبري الحديث — غانم مزعل
58. فلسطين أرض وتاريخ — د. محمد نحال
59. القدس ماضيها حاضرها ومستقبلها — فايز فهد جابر
60. القضية الفلسطينية في القانون الدولي — د. جابر الراوي
61. المؤسسة العسكرية الصهيونية في دائرة الضوء (1) إسرائيل عسكر وسلاح — بشير شريف البرغوثي
62. المؤسسة العسكرية الصهيونية في دائرة الضوء (2) أزمة الاستخبارات الإسرائيلية — تسفي لينر
63. حرب الاستنزاف (نافذ) — د. محمد حمزة
64. المطامع الإسرائيلية في مياه فلسطين — بشير البرغوثي
65. إسرائيل عام 2000 "تصورات إسرائيلية" — إعداد : قسم الدراسات
66. القرار — رشاد أحمد الصغير
67. ندوة مشاكل التعليم الجامعي في الوطن المحتل والروح الجامعية — إعداد : المجلس الأعلى للتربية والثقافة والعلوم في منظمة التحرير
68. القضية الفلسطينية — أكرم زعيتر
69. شخصيات صهيونية (1) مذكرات رفائيل ايتان — ترجمة: غازي السعدي
70. شخصيات صهيونية (2) شلومو هيلل وتهجير يهود العراق — ترجمة : غازي السعدي
71. شخصيات صهيونية (3) ثيودور هرتسل — إعداد : قسم الدراسات
72. شخصيات صهيونية (4) آرئيل شارون — عوزي بنزيمان - ترجمة : غازي السعدي

73.	شخصيات صهيونية (5) آباء الحركة الصهيونية	ترجمة : عبد الكريم النقيب
74.	شخصيات صهيونية (6) موشيه ديان	ترجمة : غازي السعدي
75.	شخصيات صهيونية (7) بن غوريون والعرب	شبتاي تيبت - ترجمة : غازي السعدي
76.	شخصيات صهيونية (8) رسائل بن غوريون	ترجمة: الأميرة دينا عبد الحميد
77.	شخصيات صهيونية (9) حياتي – لجولدا مائير	ترجمة : دار الجليل
78.	شخصيات صهيونية (10)حركة التصحيح الصهيونية	ليني برينر – ترجمة : دار الجليل
79.	شخصيات صهيونية (11) مذكرات اسحق رابين-جزآن	اسحق رابين
80.	شخصيات صهيونية (12) ناحوم غولدمان	ترجمة دار الجليل
81.	شخصيات صهيونية (13)اسحق شامير	ترجمة : دار الجليل
82.	شخصيات صهيونية (14)مكان تحت الشمس	بنيامين نتنياهو
83.	فلسطين الأم وابنها البار عبد القادر الحسيني	عيسى خليل محسن
84.	دعوى نزع الملكية	آرييه.ل.افنيري - ترجمة : بشير البرغوثي
85.	شخص غير مرغوب فيه	قصائد : سميح القاسم
86.	نادية برادلي "الفدائية المغربية الشقراء"	ترجمة : غسان كمال
87.	عرب التركمان	علياء الخطيب
88.	المرأة الفلسطينية والاحتلال الإسرائيلي	ميسون الوحيدي
89.	الإعلام الإسرائيلي	غازي السعدي ومنير الهور
90.	الوجه الحقيقي للموساد (نافذ)	د. وجيه أبو غالب وأنور خلف
91.	العمق الاستراتيجي في الحروب الحديثة	ترجمة : بدر عقيلي
92.	آه يا بلدي	أكرم النجار
93.	الحافلة رقم 300	ترجمة : احمد بركات
94.	من رواد النضال في فلسطين (1)	زياد عودة
95.	من رواد النضال في فلسطين (2)	زياد عودة
96.	من رواد النضال في فلسطين (3) (نافذ)	زياد عودة
97.	فلسطين في سيرة البطل عبد الحليم الجيلاني	د. حسن صالح عثمان
98.	الحركة العمالية في فلسطين	سليم الجنيدي

99.	الموسوعة العسكرية الإسرائيلية (1) سلاح الجو الإسرائيلي	زئيف شيف - ترجمة : دار الجليل
100.	الموسوعة العسكرية الإسرائيلية (2) سلاح الاستخبارات	عوديد غرانوت
101.	الموسوعة العسكرية الإسرائيلية (3) سلاح الهندسة	عمي شامير - ترجمة : دار الجليل
102.	الموسوعة العسكرية الإسرائيلية (4) سلاح المشاة	نتان روعي - ترجمة : دار الجليل
103.	الموسوعة العسكرية الإسرائيلية (5) سلاح المظليين	إيلان كفير
104.	الموسوعة العسكرية الإسرائيلية (6)سلاح الدروع	اريبه حشافيا
105.	معجم المصطلحات الصهيونية	إعداد افرايم ومناحيم تلمي - ترجمة : أحمد بركات
106.	حرب سيناء 56	مردخاي باراون
107.	وجه قبيح في المرآة	بروفيسور أدير كوهين
108.	تاريخ ما أهمله التاريخ (نافذ)	عبد الهادي جرار
109.	أيام الصبا	د. يوسف هيكل
110.	جلسات في رغدان	د. يوسف هيكل
111.	ربيع الحياة	د. يوسف هيكل
112.	الإعلام الفلسطيني	د. حسين أبو شنب
113.	تحت السياط	فاضل يونس
114.	دراسات في تعليم الكبار	د. عدنان أبو عمشة
115.	النزاع العربي الإسرائيلي بين فكي كماشة الدول العظمى	بقلم : موشه زاك - ترجمة : دار الجليل
116.	الغضب (نافذ)	أكرم النجار
117.	منجل في النجمة السداسية	أيسر هارئيل - ترجمة : بدر عقيلي
118.	صرخة في وجه العالم "ألبوم الانتفاضة"	إعداد : دار الجليل
119.	اشكالية الديموقراطية والبديل الإسلامي	خالد الحسن
120.	الاستخبارات والأمن القومي	ترجمة : دار الجليل
121.	الأحزاب والحكم في إسرائيل	غازي السعدي
122.	تعليم الفلسطينيين ماضيا وحاضرا ومستقبلا	الدكتور عبد القادر يوسف
123.	قبس من تراث المدينة والقرية الفلسطينية	صباح السيد عزازي
124.	اشتعالات حمدان	أكرم النجار
125.	من القمع إلى السلطة الثورية	قدري أبو بكر
126.	هذه قضيتك يا ولدي	سليم عبد العال القزق

.127	معجم الأمثال الشعبية الفلسطينية	فؤاد إبراهيم عباس – احمد عمر شاهين
.128	صناعة قرارات الأمن الوطني في إسرائيل	يهودا بن مئير - ترجمة : بدر عقيلي
.129	قمع شعب	بشير البرغوثي
.130	أسلحة وارهاب	أهارون كلايمن
.131	جليلة	أكرم النجار
.132	حدود أرض إسرائيل	البروفيسور موشيه برافر- ترجمة : بدر عقيلي
.133	الأحواز في الماضي والحاضر والمستقبل	نصار أحمد الخزعلي
.134	الفاشية الإسرائيلية	المحامي درويش ناصر
.135	الأمن القومي العربي ونظرية تطبيقه في مواجهة الأمن الإسرائيلي	العميد محمد يوسف العملة
.136	النظرية العسكرية الإسرائيلية "دفاع وهجوم"	ارئيل لفيتا
.137	خرافات يهودية (نافذ)	أحمد الشقيري
.138	دقيقتان فوق تل أبيب	محمد أزوقة
.139	سياسة إسرائيل الأمنية	زئيف كلاين ويهودا شيف – ترجمة: بدر عقيلي
.140	الهجرة اليهودية "حقائق وأرقام"	د.عمران أبو صبيح
.141	الانتفاضة	زئيف شيف وأيهود يعاري
.142	جواسيس المخابرات الإسرائيلية	يوسي ميلمان/دان رافيف- ترجمة : دار الجليل
.143	دولة إسرائيل زائلة	يعقوب شريت - ترجمة دار الجليل
.144	داود وسليمان في العهد القديم والقرآن الكريم	أحمد عيسى الأحمد
.145	الجماعة الأوروبية والقضية الفلسطينية	محمد خالد الأزعر
.146	بقايا من خبز وكتاب	أكرم النجار
.147	إسرائيل في حرب الخليج	غازي السعدي
.148	المثلث المحتوم	أحمد عز الدين بركات
.149	الاستيطان الإسرائيلي "جغرافيا وسياسيا"	اليشع ايفرات - ترجمة : دار الجليل
.150	حرب السكاكين	زياد أبو صالح ورشاد المدني
.151	انتفاضة العصافير	نجوى قعوار
.152	انهيار نظرية الأمن الإسرائيلية	أحمد بركات
.153	موسوعة عشائر وعائلات فلسطين"1" القدس مدنها وقراها	فائز أبو فردة
.154	عشيرة آل العملة "العمرو"	محمد يوسف عمرو العملة
.155	الأسرة والانتفاضة	لجنة أبحاث المرأة/نابلس
.156	قصة جاسوس00 بولارد	برنارد ر.هندرسون - ترجمة: دار الجليل
.157	أبو عجاج العينبوسي "الدكتور الثائر	عيسى خليل محسن
.158	الأسلحة الكيميائية والبيولوجية وتأثيراتها البيئية	د.عادل أحمد جرار

.159	قناع القناع	العميد محمد نور الدين شحادة
.160	تشريعات القضاء في دولة فلسطين (نافذ)	أحمد محمد المبيض
.161	الشبح	عبد الـلـه عواد
.162	دولة مجدو	عبد الـلـه عواد
.163	"هشاي" مخابرات منظمة الهجناة	إعداد دار الجليل
.164	أنساب العشائر الفلسطينية	العميد محمد يوسف العملة
.165	طرد الفلسطينيين وولادة مشكلة اللاجئين	بني موريس – ترجمة : دار الجليل
.166	الاستشراق وأبحاث الصراع لدى إسرائيل	إبراهيم عبد الكريم
.167	دليل المستوطنات الإسرائيلية في الأراضي المحتلة(1967-1991)	د.عمران أبو صبيح
.168	حرب في الخليج "أبعاد على إسرائيل"	طاقم مركز الأبحاث الاستراتيجية الإسرائيلي - يافه ترجمة: بدر عقيلي
.169	ثلاثون قضية استخبارية وأمنية في إسرائيل	يوسف أرجمان - ترجمة: دار الجليل
.170	معجم المواقع الجغرافية في فلسطين (نافذ)	قسطندي نقولا أبو حمود
.171	الشرق الأوسط الجديد	شمعون بيرس
.172	الأدب العربي في جزر البليار	عبد الرزاق حسين
.173	الأعياد والمناسبات والطقوس لدى اليهود	غازي السعدي
.174	أسلحة الدمار الشامل	وليم بوروس / روبرت ويندرم - ترجمة دار الجليل
.175	المفصل في تعلم اللغة العبرية مع الكاسيت. تعلم العبرية بدون كاسيت	بدر عقيلي
.176	القاموس العملي عبري-عربي	أمين أبو عيسى
.177	دوائر القمر	عبد الرزاق حسين
.178	أحاديث في العلم والقيم	يشعياهو ليفوفيتش- ترجمة: سلمان ناطور
.179	فلسطيني بلا هوية	صلاح خلف (أبو إياد)
.180	الحوار الفلسطيني-الأمريكي	د.محمد ربيع
.181	قرية جمزو	عطية عبد الحفيظ النجار
.182	الانقلاب السياسي في إسرائيل	أوري أزولاي ترجمة:بدر عقيلي
.183	مشكلة الأراضي في النزاع القومي بين العرب وإسرائيل منذ وعد بلفور	جاك كنو- ترجمة : محمد الدويري
.184	الموساد في العراق	شلومو نكديمون - ترجمة : بدر عقيلي
.185	دولة فلسطين-الوضع القانوني	سالم أحمد قواطين
.186	اسحق رابين-اغتيال سياسي	أمنون كبليوك - ترجمة بدر عقيلي
.187	سومخي قصة للشبيبة عن الحب والمغامرات	عاموس عوز

.188	نايف حواتمة يتحدث	نايف حواتمة
.189	سورية وإسرائيل من الحرب إلى صناعة السلام	موشيه ماعوز – ترجمة : لينا وهيب
.190	اتفاقيات أوسلو	دار الجليل
.191	الحرب الاقتصادية (100) سنة من المواجهة الاقتصادية بين اليهود والعرب	يوفال اليتسور – ترجمة: بدر عقيلي – محمد الدويري
.192	البستان – من الادب العبري	بنيامين تموز
.193	أنثولوجيا-الوجه الآخر	غرشون شكيد ودافيد سجيف – ترجمة :دار الجليل
.194	المسيرة خفايا أوسلو من الألف إلى الياء	أوري سبير كبير المفاوضين الإسرائيليين في أوسلو. ترجمة بدر عقيلي
.195	أوسلو والسلام الآخر المتوازن	نايف حواتمة
.196	أيهود باراك.. الجندي الأول	بن كسبيت وإيلان بيران -ترجمة بدر عقيلي ونور البواطلة
.197	الصهيونية .. النظرية والتطبيق	يوئيل رفيل – ترجمة : نور البواطلة
.198	الحسين والسلام (مسلسل العلاقات الاردنية – الاسرائيلية)	موشيه زاك - ترجمة دار الجليل
.199	مهنتي كرجل مخابرات "29 عاما من العمل في الشاباك"	يعقوب بيري رئيس جهاز الشاباك السابق ترجمة : بدر عقيلي
.200	أبعد من أسلو ... فلسطين الى أين	نايف حواتمة
.201	جاسوس إسرائيل في دمشق	يشيعياهو بن فورات و اوري دان – ترجمة : زكي درويش
.202	انتفاضة الأقصى 2000 الكتاب الأول قصص دامية وحكايات الشهداء	إعداد دار الجليل
.203	انتفاضة الأقصى 2000 الكتاب الثاني قصص دامية وحكايات الشهداء	إعداد دار الجليل
.204	انتفاضة الأقصى 2000 الكتاب الثالث قصص دامية وحكايات الشهداء	إعداد دار الجليل
.205	انتفاضة الأقصى 2000 الكتاب الرابع قصص دامية وحكايات الشهداء	إعداد دار الجليل
.206	انتفاضة الأقصى 2000 الكتاب الخامس قصص دامية وحكايات الشهداء	إعداد دار الجليل
.207	انتفاضة الأقصى 2000 الكتاب السادس قصص دامية وحكايات الشهداء	إعداد دار الجليل
.208	انتفاضة الأقصى 2000 الكتاب السابع قصص دامية وحكايات الشهداء	إعداد دار الجليل
.209	انتفاضة الأقصى 2000 الكتاب الثامن قصص دامية وحكايات الشهداء	إعداد دار الجليل
.210	انتفاضة الأقصى 2000 الكتاب التاسع قصص دامية وحكايات الشهداء	إعداد دار الجليل
.211	انتفاضة الأقصى 2000 الكتاب العاشر قصص دامية وحكايات الشهداء	إعداد دار الجليل

212.	آرئيل شارون (سجل خدمة وعمليات انتفامية)	ترجمة وإعداد : دار الجليل
213.	قاب قوسين أو أدنى من السلام	غلعاد شير- ترجمة: بدر عقيلي
214.	إسرائيل والقنبلة النووية	أفنر كوهين -ترجمة: بدر عقيلي
215.	فلسطين تحطم الجدار	دار الجليل
216.	الجواسيس (عشرون قضية تجسس على إسرائيل	يوسي ميلمان وايتان هابر- ترجمة: خالد أبو ستة العياصرة
217.	قضية شراء الاراضي والاستيطان االصهيوني في الأردن وحوران والجولان	دراسة وإعداد : دار الجليل
218.	الرواية الجديدة عن حرب اكتوبر "دروس في علوم الحرب وصراع الجنرالات في إسرائيل"	خالد أبو ستة
219.	الانتفاضة الاستعصاء - فلسطين الى أين	نايف حواتمة
220.	اليهودية "ديانة توحيدية أم شعب مختار"	عمر مصالحة
221.	تاريخ فلسطين قبل الميلاد	هشام أبو حاكمة
222.	انقلاب عسكري في اسرائيل - الاحتمالات والوقائع	تسفيكة عميت- ترجمة: بدر عقيلي
223.	كفاح شعب فلسطين ومسيرة حركته الوطنية	إعداد دار الجليل
224.	التلمود"المرجعيةاليهودية للتشريعات الدينية والاجتماعية"	عمر مصالحة
225.	الأساطير المؤسسة للتاريخ الاسرائيلي القديم	هشام أبو حاكمة
226.	الوعد الصادق حزب الـلـه وإسرائيل وجها لوجه	هشام ابو حاكمة
227.	رسالة الى شعب اسرائيل	محمد ابو سمرة
228.	بين العسكرية والسياسة ذكريات	عبد الرزاق اليحيى
229.	حروب الظلال الإسرائيلية وسياسة الاغتيالات	دار الجليل
230.	السلام أولا .. تحديث مسارات السلام	أوري سافير
231.	مسجد داود وليس هيكل سليمان	هشام أبو حاكمة
232.	مصطلحات ومناسبات وتواريخ وشخوص صهيونية	إعداد : دار الجليل
233.	العرب الدروز والحركة الوطنية الفلسطينية حتى ال 48	النائب سعيد نفاع
234.	النظام الانتخابي الإسرائيلي انتخابات الكنيست 2009- الأحزاب الإسرائيلية- تشكيل الحكومة- برامجها السياسية	غازي السعدي
235.	الموساد .. الشاباك.. أمان وأسلحة الدمار الشامل الإسرائيلية	دراسة/ بدر عقيلي
236.	اليسار العربي رؤيا النهوض الكبير (نقد وتوقعات)	نايف حواتمة
237.	نجوم في سماء فلسطين	زياد عودة
238.	جرائم الحرب الإسرائيلية في غزة	بدر عقيلي
239.	هدنة - أمل من أجل الشرق الأوسط	أيال آرليخ

.240	الإرهاب على فلسطين وشاهد من أهلها	مفيد المبسلط
.241	الموساد العمليات الكبرى	ميخائيل بار زوهر والصحفي نسيم مشعل ترجمة : بدر عقيلي
.242	العداء الإسرائيلي للسياسة الواقعية الفلسطينية	حمادة فراعنة
.243	العلاقات العربية – التركية	حمادة فراعنة
.244	خطاب البرنامج الفلسطيني في مواجهة المشروع الإسرائيلي	حمادة فراعنة
.245	المؤتمر السادس لحركة فتح وتداعياته	حمادة فراعنة
.246	تطورات المشهد السياسي الأردني	حمادة فراعنة
.247	المفاوضات وصلابة الموقف الفلسطيني	حمادة فراعنة
.248	موسوعة المصطلحات والمفاهيم الفلسطينية	تحرير د. محمد شتية
.249	تحديات الأمن الوطني الأردني وأثره على الاستقرار السياسي	رعد فواز الزبن
.250	الثورة الشعبية العربية "أدواتها وأهدافها" 2011	حماد فراعنة
.251	الإخوان المسلمون ودورهم السياسي	حمادة فراعنة